Copyright Notice
Copyright © 2006 Juniper Networks, Inc. All rights reserved.

Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

FCC Statement
The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with NetScreen’s installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Consult the dealer or an experienced radio/TV technician for help.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

Caution: Changes or modifications to this product could void the user’s warranty and authority to operate this device.

Disclaimer
THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR JUNIPER NETWORKS REPRESENTATIVE FOR A COPY.
Contents

About This Guide ................................................................................................. xxxvii

Audience........................................................................................................... xxxviii
Conventions...................................................................................................... xxxviii
User Interface Conventions ........................................................................... xxxviii
Illustration Conventions............................................................................... xxxix
Unsupported Characters................................................................................ xxxix

Documentation ................................................................................................ xl
NetScreen-Security Manager 2005.3 Administrator’s Guide................................. xl
Part 1: Preparing............................................................................................ xl
Part 2: Integrating............................................................................................ xli
Part 3: Managing.............................................................................................. xli
Part 4: Monitoring............................................................................................. xli
Part 5: Appendixes........................................................................................... xlii
Part 6: Index ..................................................................................................... xlii

Related Documentation .................................................................................. xliii
NetScreen-Security Manager 2005.3 Installer’s Guide.......................................... xliii
NetScreen-Security Manager 2005.3 Online Help............................................... xliii
NetScreen-Security Manager 2005.3 Release Notes............................................. xliii

Web Access..................................................................................................... xliii
Comments About the Documentation ............................................................... xliii

Contacting Customer Support .......................................................................... xliii

Part 1 Preparing

Chapter 1 Introduction to NetScreen-Security Manager ........................................... 3

About NetScreen-Security Manager 2005.3....................................................... 4
Security Integration ............................................................................................ 4
Complete Support ............................................................................................ 4
Network Organization ....................................................................................... 4
Role-Based Administration .............................................................................. 5
Centralized Device Configuration ................................................................. 5
Migration Tools................................................................................................ 6
Device Management ......................................................................................... 6
Device Modeling ............................................................................................... 6
Rapid Deployment (RD) ................................................................................... 7
Policy-Based Management ............................................................................. 7

Error Prevention, Recovery, and Auditing ......................................................... 7
Device Configuration Validation ................................................................. 8
Policy Validation ............................................................................................. 8
Atomic Configuration and Updating ............................................................. 8
Device Image Updates .................................................................................... 8
Auditing ........................................................................................................... 9

Complete System Management ..................................................................... 9
VPN Abstraction ............................................................................................ 9
Integrated Logging and Reporting ............................................................... 10
Monitoring Status.................................................................10
Job Management...............................................................10
Technical Overview...........................................................11
  Architecture..........................................................................11
  UI.......................................................................................12
  Management System.........................................................12
  Managed Device...............................................................14
Distributed Data Collection................................................15
Security..................................................................................16
Scaling and Performance.....................................................16
Working in the User Interface.................................................16
  Configuring UI Preferences................................................16
  UI Overview.........................................................................16
  Navigation Tree....................................................................17
  Main Display Area............................................................17
NetScreen-Security Manager Modules...................................17
  Log Viewer...........................................................................18
  Report Manager...............................................................18
  Log Investigator...............................................................18
  Device Manager..............................................................18
  Security Policies.............................................................19
  VPN Manager.................................................................19
  Object Manager..............................................................20
  Server Manager..............................................................21
  Realtime Monitor.............................................................21
  Job Manager.................................................................21
  Audit Log Viewer............................................................22
  Action Manager..............................................................22
Validation Icons in the User Interface.................................22
  Validation and Data Origination Icons.................................22
Working with Other NetScreen-Security Manager Administrators.23
Searching in the User Interface............................................24
  Contains String [C] Search Mode........................................24
  Starts With [S] Search Mode...............................................25
  Regular Expression [R] Search Mode....................................25
  IP [I] Search Mode..........................................................26
New Features for NetScreen-Security Manager 2005.3...............27
  Supported Security Devices and Versions of ScreenOS...........27
  NetScreen-Security Manager System and UI.........................28
    Forward Support of Future ScreenOS Releases.....................29
    Trial License Keys........................................................29
    Rule-Based Log Actions..................................................29
    Domain-Based Log Actions..............................................29
    Simplified Logs..........................................................29
    Viewing and Monitoring Devices from the Global Domain......29
    Juniper Networks Infranet Controller Support....................29
    Enhanced Certificate Support.........................................30
    Enhanced Antivirus Support............................................30
    Antispam Capabilities....................................................30
    Enhanced Template Administration..................................30
    Enhanced Deep Inspection..............................................30
    BGP Soft Reconfiguration.................................................30
    Multiple MIP Support.....................................................30
    ALG Enhancements for VoIP.............................................31
Chapter 2

Getting Started

Overview: Configuring Security Devices

- Importing Existing Devices
- Modeling New Devices

Overview: Configuring IDP-Capable Devices

- Supported IDP-Capable Devices
- Enabling IDP Functionality
  - Adding the ISG 2000 or ISG 1000 Security Device with Security Module

Maintenance and Management

- Installing License Keys
- Updating Attack Objects
- Adding Objects
- Configuring a Security Policy for IDP
- Review IDP Logs

Updating the Attack Database

- Updating the IDP Detector Engine

Creating IDP-Only Administrators

Simplifying Management

- Using Device Groups
- Using Device Templates
- Merging Policies

Using a Naming Convention

Chapter 3

Configuring Role-Based Administration

About Role-Based Administration (RBA)

- About Domains
- About Roles

Using Role-Based Administration Effectively

- Enterprise Organizations
- Geographical Divisions
- NOC and SOC
- Administrator Types

Service Providers

- Internal Network
- Managed Security Service Provider (MSSP)

Configuring Role-Based Administration

- Creating Administrators
- Configuring General Settings
- Configuring Authorization
- Configuring Permissions

Creating Roles

- Creating Custom Roles
- Assigning and Viewing Custom Roles

Creating Subdomains

- Viewing Current Domain Detail
- Domain Versioning
# Part 2

## Chapter 4

Adding Devices

- About Device Creation ................................................................. 74
- Determine Device Status .............................................................. 74
- Verify Device Configuration.......................................................... 75
- Managing the Device ................................................................. 75

Before You Begin ........................................................................ 76

- Importing vs. Modeling ............................................................... 76
  - Importing Device Configurations ............................................. 76
  - Modeling Device Configurations ............................................ 77
- Device Add Process .................................................................... 77

Selecting the Domain ................................................................... 78

- Adding Single or Multiple Devices ............................................. 79
- Determining ScreenOS Version .................................................... 80
- Determining Port Mode .............................................................. 80
  - Trust-Untrust Port Mode ......................................................... 81
  - Home-Work Port Mode ............................................................ 81
  - Dual-Untrust Port Mode ........................................................... 82
  - Combined Port Mode .............................................................. 83
  - Trust-Untrust-DMZ Port Mode .................................................. 84
  - DMZ-Dual-Untrust Port Mode .................................................. 84
  - Port Mode Summary ............................................................... 85
- Changing the Port Mode ............................................................. 86

Importing Devices........................................................................ 86

- Requirements ............................................................................ 87
- Adding Devices with Static IP Addresses .................................... 88
  - ScreenOS 4.0.x Devices .......................................................... 88
  - ScreenOS 5.x Devices ............................................................. 90
- Adding Devices with Dynamic IP Addresses ............................ 91
  - ScreenOS 4.0.x Devices .......................................................... 91
  - ScreenOS 5.x Devices ............................................................. 93

Verifying Imported Device Configurations .................................... 94

- Using Device Monitor ............................................................... 94
- Using Device Manager .............................................................. 95
- Using Job Manager ................................................................. 95
- Using Configuration Summaries ................................................ 95

Modeling Devices ...................................................................... 97

- Requirements ............................................................................ 97
- Modeling a Device ................................................................. 97
- Creating a Device Configuration ............................................... 98
- Activating a Device ................................................................. 98
  - Devices with Static IP Addresses ........................................... 98
  - Devices with Dynamic IP Addresses ................................. 101

Using Rapid Deployment ............................................................ 104

- Overview .................................................................................. 104
- Requirements .......................................................................... 105
- Creating the Configlet .............................................................. 105
  - Installing the Configlet .......................................................... 108
  - Preparing the Device ............................................................. 108
  - Installing the Configlet .......................................................... 109
- Updating the Device Configuration ....................................... 110

Adding Other Device Types ......................................................... 110
Adding Vsys Devices
Placing the Root Device
Importing Vsys Devices
Modeling Vsys Devices
Adding L2V Root Systems
Adding an Extranet Device
Adding a Cluster
Adding Members to the Cluster
Adding a Vsys Cluster and Vsys Cluster Members
Adding Many Devices
Creating the CSV File
Devices with Static IP Addresses
Device with Dynamic IP Addresses
Undeployed Devices
Validating the CSV file
Importing Many Devices
Adding Many Devices with Static IP Addresses
Adding Many Devices with Dynamic IP Addresses
Modeling Many Devices
Using Rapid Deployment
Modeling and Activating Many Devices (with Configlets)
Activating Many Devices (with Configlets)

Chapter 5 Configuring Devices

About Device Configuration
About Configuring Security Devices
About Configuring IDP-Capable Devices
About Configuring Devices Running ScreenOS 5.0 FIPS
About Configuring Devices Running Future Releases of ScreenOS
Unsupported Changes
Changes that Affect the Management Connection
Determining Device Configuration Status

Using Templates
Changing Values Set By Templates
Template Limitations
Maximum of 63 Templates
Device Groups
Default Values
Device Entities
Key List Parameters

The Template Operations Dialog
Template Operations Dialog Controls
Using the Template Operations Dialog
Step 1: Look at the effect of planned changes before making them
Step 2: Review results in job information dialog
Step 3: Apply templates and clear overrides
Removing Templates with the Template Operations Dialog

Templates and Validation
Modifying Template Values
Applying Multiple Templates
Using Device Groups
Configuring Device Information
Configuring Startup Information
Applying Templates .......................................................................................... 151
Viewing Device Capabilities ......................................................................... 151
Configuring Network Overview ..................................................................... 152
Configuring Wireless Settings ...................................................................... 153
   Configuring General Wireless Settings .................................................. 154
      Configuring Antennas ...................................................................... 154
      Configuring Channels ...................................................................... 155
   Configuring Advanced Wireless Settings ............................................... 156
      Configuring Aging ........................................................................... 157
      Configuring Beacons ....................................................................... 157
      Configuring Burst and Fragment Size .............................................. 157
      Configuring Control Frame Protection ............................................ 158
      Configuring Short Slots .................................................................. 159
      Configuring Preambles ..................................................................... 159
   Configuring Wireless MAC Access Lists ................................................. 159
      Configuring MAC Access Mode ...................................................... 160
      Configuring MAC Addresses ......................................................... 160
   Configuring Wireless SSIDs ................................................................... 160
      Configuring General SSID Settings .................................................. 161
      Configuring SSID Authentication and Encryption ............................ 161
Reactivating Wireless Connections ............................................................... 166
Conducting a Site Survey .............................................................................. 167
Configuring the Network Module ................................................................. 167
Viewing Slot Information ............................................................................. 167
   Interface Modules (Copper) .................................................................. 167
      10/100 .......................................................................................... 168
      10/100/1000 ................................................................................... 168
   Interface Modules (Fiber) ..................................................................... 168
   Secure Port Modules (SPM) .................................................................... 168
Viewing Chassis Information ......................................................................... 169
Configuring Virtual Routers .......................................................................... 169
   About Routes ....................................................................................... 170
   About Virtual Routers .......................................................................... 170
   Configuring Virtual Router General Properties ................................... 171
   Configuring Access Lists ...................................................................... 172
   Configuring Route Maps ...................................................................... 173
      Configuring Route Map Match Conditions ....................................... 173
      Configuring Permitted Route Attributes ......................................... 174
   Configuring Export and Import Rules .................................................... 175
   Configuring Routing Table Entries ....................................................... 179
      Configuring Destination-Based Routes ............................................ 180
      Configuring Source-Based Routing ................................................ 181
      Configuring Source-Interface-Based Routing ................................ 183
   Configuring Route Preferences ............................................................. 185
Configuring Dynamic Routing ..................................................................... 185
   Configuring Open Shortest Path First (OSPF) ....................................... 186
      Enabling OSPF ............................................................................... 186
      Configuring Global OSPF Settings .................................................. 187
      Configuring OSPF Interface Parameters ....................................... 189
   Configuring Routing Information Protocol (RIP) ................................. 193
      Enabling RIP ................................................................................. 193
      Configuring Global RIP Settings ..................................................... 194
      Configuring RIP Interface Parameters .......................................... 196
   Configuring Border Gateway Protocol (BGP) ....................................... 198
Configuring NACN ................................................................. 286
Configuring Interface Failover ............................................. 286
Configuring Modem Connection ........................................... 287
Creating Modem Settings ..................................................... 287
Creating ISP Settings ............................................................ 288
Setting ISP Priority for Failover ........................................... 289
Configuring DNS ................................................................. 289
Configuring DNS Settings ..................................................... 289
Configuring DNS Proxy ........................................................ 289
Configuring Dynamic DNS ................................................... 292
Configuring Advanced Network Settings ............................... 294
Configuring ARP Cache Entries ......................................... 295
Configuring VIP Options ...................................................... 295
Configuring DIP Options ...................................................... 295
Configuring Device Administration ....................................... 296
Configuring Device Administrators ....................................... 297
Configuring Authentication Servers ................................. 297
Configuring Device Administrator Accounts ....................... 298
Configuring Admin Accounts for Dialup Connections .......... 301
Configuring Permitted IPs ..................................................... 301
Configuring CLI Management .............................................. 302
Configuring the File Format ................................................. 302
Configuring SSH and Telnet Ports ....................................... 302
Configuring Connection Attempts ....................................... 303
Configuring Password Length Restriction ............................. 303
Configuring Asset Recovery and Reset Hardware .................. 303
Configuring Console-Only Connections ............................... 304
Configuring SSH ................................................................. 304
Configuring CLI Banners ..................................................... 306
Configuring Web Management ........................................... 306
Configuring HTTP ............................................................... 307
Configuring SSL ................................................................. 307
Configuring Date and Time Settings ..................................... 308
Configuring Network Time Protocol (NTP) ......................... 308
Configuring an NTP Backup Server ..................................... 309
Configuring Authentication ................................................... 309
Configuring General Auth Settings ....................................... 310
Clearing RADIUS Sessions .................................................. 310
Assigning an Authentication Request Interface .................... 310
Configuring Banners .......................................................... 311
Configuring Default Servers .............................................. 311
Configuring an Auth Server ............................................... 312
Configuring a WebAuth Server ............................................ 312
Configuring Infranet Settings .............................................. 312
Configuring Reporting ......................................................... 313
Configuring General Reporting Settings ......................... 313
Configuring Email Notification Settings ............................ 313
Configuring NetScreen-Security Manager Reporting ............ 314
Configuring SNMP Reporting ............................................ 314
Configuring Syslog Reporting ............................................. 314
Configuring a Syslog Host .................................................. 314
Configuring Webtrends Reporting ..................................... 315
Configuring Security .......................................................... 315
Configuring AntiVirus (AV) Settings ................................. 315
<table>
<thead>
<tr>
<th>Contents</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring External AV Scanners</td>
<td>316</td>
</tr>
<tr>
<td>Configuring the Internal AV Scanner</td>
<td>317</td>
</tr>
<tr>
<td>Configuring AV HTTP Webmail Settings</td>
<td>318</td>
</tr>
<tr>
<td>Configuring AV Scanner Settings</td>
<td>319</td>
</tr>
<tr>
<td>Configuring Antispam</td>
<td>320</td>
</tr>
<tr>
<td>Configuring Antispam Settings for a Device</td>
<td>321</td>
</tr>
<tr>
<td>Configuring Web Filtering</td>
<td>322</td>
</tr>
<tr>
<td>Configuring Integrated Web Filtering</td>
<td>323</td>
</tr>
<tr>
<td>Redirect Web Filtering</td>
<td>324</td>
</tr>
<tr>
<td>Configuring Deep Inspection</td>
<td>326</td>
</tr>
<tr>
<td>Configuring the Attack Database</td>
<td>327</td>
</tr>
<tr>
<td>Disabling Attack Objects</td>
<td>328</td>
</tr>
<tr>
<td>Configuring Security Module (SM) Settings</td>
<td>328</td>
</tr>
<tr>
<td>Configuring Load Time Parameters</td>
<td>329</td>
</tr>
<tr>
<td>Configuring Run-Time Parameters</td>
<td>329</td>
</tr>
<tr>
<td>Configuring Protocol Thresholds</td>
<td>330</td>
</tr>
<tr>
<td>Configuring Advanced Device Settings</td>
<td>330</td>
</tr>
<tr>
<td>Configuring Timeouts for Predefined Services</td>
<td>331</td>
</tr>
<tr>
<td>Configuring SIP Settings</td>
<td>331</td>
</tr>
<tr>
<td>Setting SIP Inactivity Timeouts</td>
<td>332</td>
</tr>
<tr>
<td>Configuring SIP Firewall Features</td>
<td>332</td>
</tr>
<tr>
<td>Configuring MGCP Settings</td>
<td>333</td>
</tr>
<tr>
<td>Setting MGCP Inactivity Timeouts</td>
<td>333</td>
</tr>
<tr>
<td>Configuring MGCP Firewall Features</td>
<td>333</td>
</tr>
<tr>
<td>Configuring H.323 Settings</td>
<td>334</td>
</tr>
<tr>
<td>Setting H.323 Inactivity Timeouts</td>
<td>334</td>
</tr>
<tr>
<td>Configuring Traffic Shaping</td>
<td>334</td>
</tr>
<tr>
<td>Configuring Application Layer Gateways (ALGs)</td>
<td>335</td>
</tr>
<tr>
<td>Configuring Packet Flow</td>
<td>336</td>
</tr>
<tr>
<td>ICMP Path MTU Discovery</td>
<td>337</td>
</tr>
<tr>
<td>Allow DNS Reply Without Matched Request</td>
<td>337</td>
</tr>
<tr>
<td>Allow MAC Cache for Management Traffic</td>
<td>338</td>
</tr>
<tr>
<td>Allow Unknown MAC Flooding</td>
<td>338</td>
</tr>
<tr>
<td>Skip TCP Sequence Number Check</td>
<td>338</td>
</tr>
<tr>
<td>TCP RST Invalid Session</td>
<td>339</td>
</tr>
<tr>
<td>Check TCP SYN Bit Before Create Session</td>
<td>339</td>
</tr>
<tr>
<td>Check TCP SYN Bit Before Create Session for Tunneled Packets</td>
<td>339</td>
</tr>
<tr>
<td>Use SYN-Cookie for SYN Flood Protection</td>
<td>339</td>
</tr>
<tr>
<td>Enforce TCP Sequence Number Check on TCP RST Packet</td>
<td>340</td>
</tr>
<tr>
<td>Use Hub-and-Spoke Policies for Untrust MIP Traffic</td>
<td>340</td>
</tr>
<tr>
<td>Max Fragmented Packet Size</td>
<td>341</td>
</tr>
<tr>
<td>Flow Initial Session Timeout (Seconds)</td>
<td>341</td>
</tr>
<tr>
<td>TCP MSS</td>
<td>341</td>
</tr>
<tr>
<td>All TCP MSS</td>
<td>341</td>
</tr>
<tr>
<td>GRE In TCP MSS</td>
<td>342</td>
</tr>
<tr>
<td>GRE Out TCP MSS</td>
<td>342</td>
</tr>
<tr>
<td>Ageing</td>
<td>342</td>
</tr>
<tr>
<td>Configuring Supplemental Command Line Interface (CLI)</td>
<td>343</td>
</tr>
<tr>
<td>Configuring TFTP/FTP Server Operation</td>
<td>343</td>
</tr>
<tr>
<td>Configuring Host and Domain Name</td>
<td>344</td>
</tr>
<tr>
<td>Configuring NSGP</td>
<td>344</td>
</tr>
<tr>
<td>About Overbilling</td>
<td>345</td>
</tr>
<tr>
<td>Configuring L2TP and XAuth Local Users</td>
<td>349</td>
</tr>
<tr>
<td>Configuring L2TP Local Users</td>
<td>349</td>
</tr>
</tbody>
</table>
Contents

About XAuth Users ................................................................................351
Configuring vsys ..................................................................................351
Viewing Root and Vsys Configurations ..............................................352
Configuring Virtual Routers for Root and Vsys.................................352
Configuring Zones for Root and Vsys..................................................353
Configuring Interfaces for Root and Vsys...........................................353
Using the VLAN Management Interface .........................................354
Routing Traffic to Vsys........................................................................354
Using VLAN IDs..................................................................................354
Using IP Classification .......................................................................357
Configuring Layer 2 Vsys (L2V)..............................................................359
Assigning L2V VLAN IDs..................................................................359
Creating L2V VLAN Groups...............................................................360
Configuring L2V Zones......................................................................360
Configuring L2V Interfaces...............................................................361
Converting L2V to VLAN Trunking.......................................................362
Configuring Certificates........................................................................366
Using Self-Signed Certificates (ScreenOS 5.1 and Higher Only)..............366
Configuring A Local Certificate..............................................................367
Generating the Certificate Request......................................................367
Obtaining and Installing the Local Certificate (CA or SCEP Only)....369
Installing the Local Certificate Using SCEP........................................370
Installing the Local Certificate Manually..........................................370
Configuring CA Certificates.................................................................371
Obtaining and Installing a CA Certificate Using SCEP....................371
Obtaining and Installing a CA Certificate Manually..........................371
Configuring CRLs................................................................................372
Using Imported Certificates..................................................................373
Configuring PKI Defaults ...................................................................373
Configuring X509 Certificates .............................................................373
Configuring Revocation.....................................................................374
Configuring SCEP...............................................................................375
Configuring NSRP Clusters ....................................................................376
About NSRP Clusters............................................................................376
Creating an NSRP Cluster ................................................................377
Active/Passive Configurations...............................................................378
Active/Active Configurations...............................................................381
Synchronizing Configurations..............................................................382
Synchronizing the Virtual Router.......................................................382
Synchronizing Run-Time Objects (RTOs)...........................................383
Forcing VSD Group Member State.......................................................383
Configuring Monitoring (For Failover)..................................................385
Configuring Track IPs.........................................................................386
Configuring Interface Monitoring.........................................................386
Configuring Zone Monitoring..............................................................387
Configuring Monitor Threshold............................................................387
Configuring Vsys Clusters....................................................................387
Exporting and Importing Device Configurations...............................388

Chapter 6  Updating Devices .................................................................389
About Updating..................................................................................390
The Update Lifecycle ........................................................................391
About Atomic Configuration (ScreenOS 5.x Only).................................392
About Atomic Updating (ScreenOS 5.1 or Higher Only)......................392
Setting RMA State on a Device ............................................................... 430
Troubleshooting a BGP Peer Session on a Device ............................. 430
Displaying CLI Commands on a Device .......................................... 431
 Reactivating Wireless Connections .................................................. 431
Finding Usages .................................................................................. 431
Managing Device Capabilities ........................................................... 431
Abstract Data Model ........................................................................ 432
Data Model ........................................................................................ 432
  Data Model Schema ...................................................................... 433
  Data Model Updating .................................................................... 433
  Data Model Importing .................................................................. 435
Archiving and Restoring .................................................................. 436
  Archiving Logs and Configuration Data ........................................ 436
  Restoring Logs and Configuration Data ........................................ 437

Part 3  Managing

Chapter 8  Configuring Objects ......................................................... 441
About Objects ..................................................................................... 442
  Importing Objects from Global-PRO .............................................. 443
  Using Objects Across Domains .................................................... 443
Configuring Address Objects ............................................................ 444
  Viewing Address Objects .............................................................. 444
  Creating Address Objects ............................................................. 445
    Adding a Host Address Object .................................................... 445
    Adding a Network Address Object ............................................. 445
    Adding an Address Object Group ............................................. 446
    Adding a Multicast Group Address Object ............................... 446
    Adding Static DNS Host Addresses .......................................... 447
Configuring Schedule Objects .......................................................... 448
  Creating Schedule Objects ............................................................ 449
Working With DI Attack Objects ....................................................... 449
  Viewing Predefined DI Attack Objects ........................................ 450
  Viewing Attack Version Information for Attack Objects .............. 450
  Viewing Predefined DI Attack Object Groups ............................. 450
Updating Predefined DI Attack Objects and Groups ......................... 451
  Creating DI Profiles ..................................................................... 451
Working with IDP Attack Objects ....................................................... 453
  Viewing Predefined IDP Attacks ................................................ 453
  Viewing Predefined IDP Attack Groups ....................................... 455
  Viewing Attack Version Information for Attack Objects and Groups 455
  Updating Predefined IDP Attack Objects and Groups ................ 455
 Configuring Custom DI/IDP Attacks ................................................... 456
  Using the Attack Object Wizard .................................................. 456
    Configuring Attack Name and Description ............................... 457
    Configuring Extended Information ......................................... 458
    Configuring External References .......................................... 458
    Configuring Target Platforms ................................................. 459
    Creating a Signature Attack Object ....................................... 460
    Configuring General Attack Properties ................................. 460
    Configuring Attack Detection Properties ............................... 464
## Contents

- Configuring Header Match Properties..............................................467
- Configuring a Protocol Anomaly Attack Object ......................................470
- Configuring a Compound Attack Object .................................................471
- Configuring General Attack Properties .............................................472
- Configuring Compound Attack Members ........................................472
- Configuring Direction Filter ...................................................................473
- Creating Custom DI Attack Groups...............................................................474
- Creating Custom IDP Attack Groups.............................................................474
- Creating Static Attack Groups ............................................................474
- Creating Dynamic Attack Groups (IDP Only)..........................................475
- Updating Dynamic Groups.....................................................................477
- Editing a Custom Attack Group..............................................................478
- Deleting a Custom Attack Group............................................................478
- Configuring AntiVirus Objects ......................................................................478
- Configuring External AV Profiles............................................................478
- Configuring Internal AV Profiles ............................................................479
  - View the Predefined Profile....................................................................479
  - Create Custom AV Profiles.......................................................................479
  - Configuring Extension Lists......................................................................480
- Configuring Web Filtering Objects ...............................................................481
  - URL Categories ......................................................................................481
  - Custom Lists ...........................................................................................482
  - Predefined Categories ...........................................................................483
  - URL Profiles ..........................................................................................484
  - Custom Profiles .........................................................................................484
  - Predefined Profiles ...................................................................................485
- Configuring GTP Objects ..............................................................................486
  - Configuring Info ....................................................................................486
    - Limiting GTP Message Length .........................................................486
    - Limiting GTP Message Rate..............................................................486
    - Limiting GTP Tunnels.....................................................................487
    - Removing Inactive GTP Tunnels......................................................487
    - Validating Sequence Numbers .......................................................487
    - Filtering GTP-in-GTP Packets...........................................................488
  - Configuring Traffic Logging and Counting..............................................488
    - Traffic Counting ...............................................................................488
    - Traffic Logging ..................................................................................488
  - Configuring IMSI Prefix and APN Filtering .............................................489
    - Creating an APN Filter .....................................................................489
    - Creating an IMSI Prefix Filter ..........................................................490
  - Configuring GTP Message Filtering .........................................................490
  - Configuring Subscriber Tracing (Lawful Interception) ............................490
  - Configuring Service Objects .........................................................................492
    - Viewing Predefined Services ..........................................................492
    - Configuring Custom Services ..........................................................494
    - Service Object Groups .......................................................................495
  - Configuring Authentication Servers .........................................................498
    - Configuring General Authentication Server Settings .........................499
    - Configuring Authentication Server Redundancy ..................................499
    - Configuring Authentication for User Types ..........................................499
    - Domain Name Checking ....................................................................500
    - Domain Name Striping ......................................................................500
    - Configuring Authentication Server Types ..........................................500
    - Configuring a RADIUS Authentication Server ....................................501
<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>505</td>
</tr>
<tr>
<td>506</td>
</tr>
<tr>
<td>507</td>
</tr>
<tr>
<td>507</td>
</tr>
<tr>
<td>507</td>
</tr>
<tr>
<td>508</td>
</tr>
<tr>
<td>508</td>
</tr>
<tr>
<td>511</td>
</tr>
<tr>
<td>511</td>
</tr>
<tr>
<td>512</td>
</tr>
<tr>
<td>513</td>
</tr>
<tr>
<td>515</td>
</tr>
<tr>
<td>516</td>
</tr>
<tr>
<td>516</td>
</tr>
<tr>
<td>516</td>
</tr>
<tr>
<td>516</td>
</tr>
<tr>
<td>517</td>
</tr>
<tr>
<td>518</td>
</tr>
<tr>
<td>518</td>
</tr>
<tr>
<td>520</td>
</tr>
<tr>
<td>520</td>
</tr>
<tr>
<td>520</td>
</tr>
<tr>
<td>520</td>
</tr>
<tr>
<td>522</td>
</tr>
<tr>
<td>522</td>
</tr>
<tr>
<td>523</td>
</tr>
<tr>
<td>524</td>
</tr>
<tr>
<td>524</td>
</tr>
<tr>
<td>527</td>
</tr>
<tr>
<td>528</td>
</tr>
<tr>
<td>528</td>
</tr>
<tr>
<td>529</td>
</tr>
<tr>
<td>530</td>
</tr>
<tr>
<td>530</td>
</tr>
<tr>
<td>530</td>
</tr>
<tr>
<td>531</td>
</tr>
<tr>
<td>531</td>
</tr>
<tr>
<td>532</td>
</tr>
<tr>
<td>532</td>
</tr>
<tr>
<td>533</td>
</tr>
<tr>
<td>533</td>
</tr>
<tr>
<td>534</td>
</tr>
<tr>
<td>534</td>
</tr>
<tr>
<td>534</td>
</tr>
<tr>
<td>535</td>
</tr>
<tr>
<td>536</td>
</tr>
<tr>
<td>536</td>
</tr>
<tr>
<td>537</td>
</tr>
<tr>
<td>537</td>
</tr>
<tr>
<td>537</td>
</tr>
<tr>
<td>537</td>
</tr>
<tr>
<td>540</td>
</tr>
<tr>
<td>541</td>
</tr>
</tbody>
</table>
Configuring Firewall Rule Options .........................................................542
   Enabling NAT ..................................................................................542
   Enabling GTP for Firewall Rules ......................................................543
   Configuring Traffic Shaping in a Security Policy ..............................543
   Enabling Logging and Counting for Firewall Rules...........................545
   Miscellaneous..................................................................................546
   ID ....................................................................................................547
   Configuring WEB Filtering for Firewall Rules...................................548
   Configuring Authentication For Firewall Rules..................................550
   Configuring AntiVirus For Firewall Rules .........................................551
   Configuring a DI Profile/Enable IDP For Firewall Rules....................551
   Comments For Firewall Rules..........................................................553
Configuring Multicast Rules.................................................................553
   Configuring Source and Destination Zones ............................................553
   Configuring Source and Destination Groups ..........................................554
   Configuring Rule Options...................................................................554
Configuring Antivirus Rules..........................................................................555
Configuring Antispam Rules.........................................................................556
Configuring IDP Rules..................................................................................556
   Defining Match For IDP Rules..........................................................557
   Configuring Source & Destination Zones for IDP Rules ..............557
   Configuring Source & Destination Address Objects for IDP Rules 557
   Configuring Services for IDP Rules ..................................................558
   Configuring Terminal IDP Rules ......................................................561
   Defining Actions For IDP Rules..........................................................562
   Configuring Attack Objects in IDP Rules ...........................................563
   Adding IDP Attack Object Groups by Category ................................564
   Adding IDP Attack Objects by Operating System .............................564
   Adding IDP Attack Objects by Severity .............................................564
   Adding Custom Dynamic Attack Groups ..........................................565
   Configuring IP Actions in IDP Rules...................................................565
   Choosing an IP Action......................................................................565
   Choosing a Block Option...................................................................565
   Setting Logging Options ..................................................................566
   Setting Timeout Options ..................................................................566
   Configuring Notification in IDP Rules.................................................566
   Setting Severity for IDP Rules ..........................................................567
   Setting Target Security Devices for IDP Rules ...............................567
   Entering Comments for IDP Rules ....................................................567
Configuring Exempt Rules............................................................................568
   Adding the Exempt Rulebase .............................................................569
   Defining Match................................................................................569
   Configuring Source & Destination Zones ..........................................570
   Configuring Source & Destination Address Objects ...........................570
   Setting Attack Objects......................................................................570
   Setting Targets................................................................................571
   Entering Comments..........................................................................571
   Creating an Exempt Rule from the Log Viewer ................................571
Configuring Backdoor Rules........................................................................572
   Adding the Backdoor Rulebase ........................................................573
   Defining Match................................................................................573
   Configuring Source & Destination Zones ..........................................574
   Configuring Source & Destination Address Objects ...........................574
   Configuring Services .......................................................................574
Setting Operation ................................................................. 574
Setting Actions .............................................................................. 574
Setting Notification ...................................................................... 575
  Setting Logging ........................................................................ 575
  Setting an Alert ...................................................................... 575
  Logging Packets ...................................................................... 576
Setting Severity .......................................................................... 576
Setting Targets ........................................................................... 576
Entering Comments ...................................................................... 576
Installing Security Policies .......................................................... 576
  Assigning a Security Policy to a Device .................................... 577
Validating Security Policies .......................................................... 577
  Rule Shadowing ...................................................................... 578
Unsupported Options ..................................................................... 579
Installing New Security Policies .................................................... 579
Updating Existing Security Policies ................................................ 581
Managing Rules and Policies ....................................................... 582
  Helpful Tips ............................................................................ 582
Using Zone Exceptions ............................................................... 583
Using Zone Filters ....................................................................... 584
Selecting Rules ........................................................................... 584
Editing Rule Order ....................................................................... 584
Using Cut, Copy, and Paste .......................................................... 585
Deleting a Rule ............................................................................ 585
Disabling a Rule .......................................................................... 585
Using Rule Groups ...................................................................... 585
Re-Importing Devices & Security Policies ........................................ 586
Merging Policies .......................................................................... 586
Exporting Policies ........................................................................ 589

Chapter 10 Configuring VPNs ...................................................... 591
About VPNs ................................................................................. 592
  Creating System-Level VPNs with VPN Manager ......................... 592
  Creating Device-Level VPNs in Device Manager ......................... 593
Supported VPN Configurations .................................................... 593
Planning for Your VPN ............................................................... 593
  Determining Your VPN Members and Topology ......................... 594
    Using Network Address Translation (NAT) ................................. 594
    Site-to-Site .......................................................................... 594
    Hub and Spoke ..................................................................... 595
    Full Mesh ............................................................................ 596
  Creating Redundancy ................................................................ 597
Protecting Data in the VPN .......................................................... 597
  Using IPSec ............................................................................ 597
  Using L2TP ............................................................................ 599
Choosing a VPN Tunnel Type ....................................................... 600
  About Policy-Based VPNs ....................................................... 600
  About Route-Based VPNs ....................................................... 601
VPN Checklist ............................................................................ 601
  Define Members and Topology ................................................. 601
  Define VPN Type: Policy-Based, Route-Based, or Mixed-Mode ...... 601
  Define Security Protocol (Encryption and Authentication) .......... 602
  Define Method: VPN Manager or Device-Level? ....................... 602
Preparing VPN Components ....................................................... 604
### Preparing Basic VPN Components ......................................................... 604
- Preparing Required Policy-Based VPN Components .............................. 604
  - Configuring Address Objects ........................................................... 605
  - Configuring Protected Resources ..................................................... 605
  - Configuring Shared NAT Objects ..................................................... 605
  - Configuring Remote Access Service (RAS) Users ............................. 606
- Configuring Required Routing-Based VPN Components ......................... 608
  - Configuring Tunnel Interfaces and Tunnel Zones ............................ 608
- Configuring Static and Dynamic Routes .......................................... 609
- Configuring Optional VPN Components................................................. 609
  - Creating Authentication Servers .................................................. 609
  - Creating Certificate Objects ....................................................... 609
  - Creating PKI Defaults ................................................................ 611
### Creating VPNs with VPN Manager .................................................... 611
- Adding the VPN ..................................................................................... 611
- Configuring Members ............................................................................ 612
  - Adding Policy-Based Members ...................................................... 612
  - Adding RAS Users ........................................................................... 615
  - Adding Routing-Based Members .................................................... 615
- Configuring Topology ............................................................................ 616
  - Configuring Common VPN Topologies ............................................ 617
  - Defining Termination Points .......................................................... 618
- Configuring Gateways ............................................................................ 618
  - Configuring Gateway Properties .................................................... 618
  - Configuring Gateway Security ....................................................... 620
  - Configuring IKE IDs ........................................................................ 621
- Configuring IKE ..................................................................................... 622
  - IKE Properties .................................................................................. 622
  - Configuring Security Level ............................................................. 623
- Autogenerating VPN Rules ..................................................................... 624
- Configuring Overrides ........................................................................... 624
  - Editing Policy Rules ........................................................................ 624
  - Editing Device Configuration .......................................................... 625
  - Viewing the Device Tunnel Summary ............................................. 626
- Adding the VPN Link ............................................................................. 626
- Editing VPNs .......................................................................................... 626
  - Editing VPN Protected Resources .................................................. 627
  - Editing Users .................................................................................... 627
  - Editing the VPN Configuration ....................................................... 627
  - Editing VPN Overrides .................................................................... 627
### VPN Manager Examples ........................................................................ 627
- Creating Device-Level VPNs .................................................................. 650
- Supported Configurations ..................................................................... 650
- Creating AutoKey IKE VPNs .................................................................. 651
  - Configuring Gateways ..................................................................... 651
  - Configuring Routes (Route-based only) ........................................... 655
  - Configuring the VPN ....................................................................... 656
  - Adding a VPN Rule .......................................................................... 658
- Creating Manual Key VPNs .................................................................. 658
  - Adding XAuth Users ........................................................................ 659
  - Configuring Routes (Route-based only) ........................................... 659
  - Configuring the VPN ....................................................................... 659
  - Adding a VPN Rule .......................................................................... 661
- Creating L2TP VPNs ............................................................................. 662
Part 4 Monitoring

Chapter 11 Monitoring 681

About the Realtime Monitor ............................................................... 681
Realtime Monitor Views .................................................................. 682
Monitoring Security Devices ............................................................ 682
Viewing Device Status .................................................................. 683
Device Polling Intervals .................................................................. 685
Viewing Additional Device Detail and Statistics .............................. 686
Viewing Device Details .................................................................. 686
Viewing Device Statistics ............................................................... 688
Monitoring VPNs .......................................................................... 706
Viewing the VPN Status Summary .................................................. 707
Configuring a VPN Display Filter .................................................... 708
Viewing Active VPN Details ........................................................... 708
Viewing Device-Specific VPN Information ...................................... 708
Monitoring NSRP Statistics ............................................................. 708
Viewing NSRP Summary Information ............................................. 708
Viewing VSD/RTO Information ....................................................... 709
Viewing VSD Counter Details ........................................................ 710
Viewing RTO Counter Details ....................................................... 710
Using The Realtime Monitor .......................................................... 711
Monitoring the Management System ................................................. 711
Configuring Servers .................................................................... 711
Configuring Device Servers .......................................................... 712
Configuring the GUI Server .......................................................... 713
Using Server Monitor .................................................................... 713
Viewing Server Status .................................................................. 713
Viewing Additional Server Status Details ...................................... 714
Viewing Process Status ................................................................. 716

Chapter 12 Logging 719

About Logging .............................................................................. 720
About Log Entries .......................................................................... 720
About Log Events .......................................................................... 720
About Log Categories .................................................................... 721
About Log Severity ........................................................................ 722
Viewing Logs .............................................................................. 723
Configuring Logging ..................................................................... 723
Configuring the Device for Logging ................................................. 724
Configuring Severity Settings .......................................................... 724
Configuring Email Server Settings .................................................... 726
Configuring Events Reporting Settings .......................................... 726
Configuring SNMP Reporting Settings ........................................... 732
Directing Logs to a Syslog Server .................................................. 733
Directing Data to a WebTrends Server .......................................... 734
Using the Log Viewer ........................................................................ 734
About the Log Viewer UI ............................................................... 735
Log Viewer Columns ..................................................................... 736
Log Viewer Detail Panes ............................................................... 739
Log Viewer Status Bar .................................................................. 739
Navigating the Log Viewer ........................................................... 740
Searching Log Entries ..................................................................... 740
Log Timeline .................................................................................. 741
Using Flags .................................................................................. 743
Using the Find Utility ................................................................. 744
Using Log ID Number .................................................................. 744
Filtering Log Entries by Event and Time ........................................ 744
Setting a Category Filter .............................................................. 745
Setting an Alert Filter .................................................................. 745
Setting a Flag Filter ..................................................................... 746
Setting an Address Filter ............................................................ 746
Setting a Protocol Filter ............................................................... 746
Setting a Domain Filter ............................................................... 746
Setting a Time-Based Filter .......................................................... 746
Filtering Log Entries by Range ..................................................... 747
Setting a Bytes In/Out Range Filter .............................................. 747
Setting a Port Number Range Filter ............................................. 748
Customizing Columns .................................................................... 748
Using Column Settings ............................................................... 749
Hide/Unhide/Move Columns .......................................................... 749
Using Log Views ........................................................................... 750
Creating Custom Views ............................................................... 751
Exporting Views .......................................................................... 751
Using Log Viewer Integration .......................................................... 751
Jump to Policy ............................................................................. 752
Jump to Device Configuration ....................................................... 752
Identifying Irrelevant Attacks ........................................................... 753
Using the Log Investigator ............................................................... 754
About the Log Investigator UI ......................................................... 754
Configuring Log Investigator Options ........................................ 756
Configuring a Time Period ............................................................. 756
Configuring Axes ........................................................................ 757
Setting a Log Entry Limit ............................................................... 759
Setting Log Investigator Filters ...................................................... 759
Investigating Log Entry Data ........................................................... 761
Using Rows and Columns ............................................................... 761
Using Cells .................................................................................. 762
Zoom Details .................................................................................. 763
Jumping to the Log Viewer ............................................................. 764
Excluding Data ............................................................................. 764
Using the Audit Log Viewer ............................................................. 764
Audit Log Table ........................................................................... 765
Target View and Device View .......................................................... 766
NetScreen-Security Manager 2005.3 Administrator's Guide

Setting a Start Time for Audit Log Entries .............................................. 766
Audit Log Entry Actions ......................................................................... 766
Managing Log Volume ........................................................................... 768
Archiving Logs ..................................................................................... 768
Purging Logs ......................................................................................... 769
Forwarding Logs ................................................................................... 769
Using the Action Manager to Forward Logs by Domain ......................... 770
    Configuring Action Parameters ......................................................... 770
    Setting Device Action Log Criteria .................................................... 772
Using the Log2Action Utility to Export Logs ........................................... 773
    Using Filters ..................................................................................... 773
    Exporting to XML ........................................................................... 775
    Using XML Required/Optional Format-Specify Filters ....................... 775
    Viewing XML Format Output .............................................................. 775
    Exporting to CSV ........................................................................... 775
    Using CSV Required/Optional Format-Specify Filters ....................... 776
    Viewing CSV Format Output .............................................................. 776
    Exporting to SNMP .......................................................................... 776
    Using SNMP Required/Optional Format-Specify Filters ..................... 777
    Viewing SNMP Format Output ............................................................ 777
    Exporting to Email ........................................................................... 777
    Using Email Required/Optional Format-Specify Filters ..................... 778
    Exporting to syslog ........................................................................... 778
    Using Syslog Required/Optional Format-Specify Filters ..................... 778
    Viewing Syslog Format Output ............................................................ 779
    Exporting to a Script ........................................................................ 779
    Using Script Required/Optional Format-Specify Filters ..................... 780

Chapter 13 Reporting ............................................................................. 781

About Reporting ..................................................................................... 782
    Report Type Groupings ..................................................................... 782
    Graphical Data Representation ......................................................... 783
    Integration with Logs ........................................................................ 783
    Central Access to Management Information ....................................... 783
Report Types .......................................................................................... 783
    Predefined Reports .......................................................................... 783
    FW/VPN Reports .............................................................................. 784
    DI/IDP Reports .................................................................................. 784
    Screen Reports .................................................................................. 785
    Administrative Reports ...................................................................... 785
My Reports .............................................................................................. 786
    Shared Reports .................................................................................. 786
Working With Reports ............................................................................. 786
    Generating a Pre-Defined Report ....................................................... 786
    Creating a Custom Report ................................................................. 787
    Generating Reports Automatically ..................................................... 788
    Using Cron with Scheduled Reports ................................................ 789
    Deleting Reports ................................................................................ 790
    Exporting Reports to HTML ............................................................... 790
Setting Report Options ........................................................................... 790
    Naming a Report ................................................................................ 791
    Setting the Report Type ..................................................................... 791
    Configuring Report Source Data ....................................................... 791
    Configuring a Report Time Period ..................................................... 791
List of Figures

Figure 1: UI Navigation Example ........................................................... xxxviii
Figure 2: Graphic Conventions................................................................. xxxix
Figure 1: NetScreen-Security Manager Network Architecture..................... 11
Figure 2: NetScreen-Security Manager System Architecture........................ 12
Figure 3: Overview of the User Interface ...................................................... 17
Figure 4: UI Search Modes............................................................................ 24
Figure 5: “Contains String” Search Mode Example ....................................... 25
Figure 6: “Starts With” Search Mode Example.............................................. 25
Figure 7: “Regular Expression” Search Mode Details .................................... 26
Figure 8: “Regular Expression” Search Mode Example .................................. 26
Figure 9: “IP Address” Search Mode Example .............................................. 27
Figure 10: New Role Dialog Box ................................................................. 68
Figure 11: Manage Administrators and Domains: Administrators Tab .......... 69
Figure 12: Device Add Process .................................................................... 78
Figure 13: Connecting Devices from Different Domains in VPNs................ 79
Figure 14: Trust-Untrust Port Mode Bindings .............................................. 81
Figure 15: Home-Work Port Mode Bindings ............................................... 82
Figure 16: Dual-Untrust Port Mode Bindings .............................................. 82
Figure 17: Combined Port Mode Bindings ................................................... 83
Figure 18: Trust-Untrust-DMZ Port Mode Bindings.................................. 84
Figure 19: DMZ Dual Untrust Port Mode..................................................... 85
Figure 20: Connecting Vsys Devices Across Domains................................ 111
Figure 21: Configuring Cluster Members for Paris Vsys Cluster............... 118
Figure 22: Paris Cluster Members and Paris Vsys Cluster Members .......... 119
Figure 23: View Template Override Message............................................. 134
Figure 24: Revert to a Template or Default Value ...................................... 134
Figure 25: Template Operations Dialog .................................................... 138
Figure 26: Select Template Dialog ............................................................ 139
Figure 27: Template Operations Job Information Dialog............................ 141
Figure 28: View Denial of Service Defense Values from DoS Template .... 145
Figure 29: Configure DoS Defense Settings for the DoS2 Template .......... 146
Figure 30: View Template Priority (DoS Highest) ....................................... 146
Figure 31: Set Template Priority (DoS2 Highest) ......................................... 147
Figure 32: View Values from DoS and DoS2 Templates................................. 147
Figure 33: View DoS2 Value for Source IP Based Session Limit ................ 148
Figure 34: View DoS Value for SYN-ACK-ACK Proxy Protection Setting .... 148
Figure 35: View Default SYN-ACK-ACK Proxy Protection Setting ........... 148
Figure 36: Using the NetScreen-5GT Wireless as a WAP ............................ 154
Figure 37: Configure New Route Map for an Export Rule......................... 176
Figure 38: Configure New Route Map for an Auto-Export Route ............... 178
Figure 39: Source-Based Routing Example Overview.................................. 181
Figure 40: Confirm Entries for Source-Based Routing Table....................... 182
Figure 41: Source Interface-Based Routing Overview................................ 184
Figure 42: Configure IGMP on an Interface.............................................. 207
Figure 43: Configure Multicast Group....................................................... 208
Figure 44: Configure Access List for Multicast Group ................................ 208
Figure 45: Create RIP Instance on Virtual Router ..................................... 208
Figure 46: Create PIM-SM Instance on Virtual Router .............................. 209
Figure 47: Configure Unicast and Multicast Data Traffic ........................... 209
Figure 48: Configure Multicast Rule to Permit PIM-SM Messages ..................209
Figure 49: View Custom Options for DHCP Server ........................................229
Figure 50: Configure MIP on Untrust Interface ..............................................231
Figure 51: Configure Global MIP ...................................................................233
Figure 52: Configure Firewall Rule to Use Global MIP ...................................233
Figure 53: Configure VIP Example Overview ................................................235
Figure 54: Configure Global VIP ...................................................................236
Figure 55: Configure a Firewall Rule to Use a Global VIP ..............................236
Figure 56: Configure Tunnel Interface ..........................................................238
Figure 57: Using DIP in Different Subnets Example Overview ......................240
Figure 58: Configure Global DIP for Office A and Office B DIPs .................243
Figure 59: Configure Two Firewall Rules to Use Global DIP .......................244
Figure 60: Configure Interface DIP Example Overview ...............................245
Figure 61: Configure Global DIP for Interface DIP ........................................246
Figure 62: Configure Rules with Interface DIP for Incoming SIP Traffic .........247
Figure 63: Configuring DIP Pool for SIP Example Overview .........................247
Figure 64: Configure Global DIP for Incoming NAT DIP Pool .......................249
Figure 65: Configure Rules with Incoming DIP Traffic for SIP .....................249
Figure 66: Redundant Interfaces for VSIs ....................................................254
Figure 67: Tunnel Interface Overview ...........................................................259
Figure 68: Access Internet Through ADSL Interface ....................................264
Figure 69: Configure Global MIP .................................................................266
Figure 70: Create New Firewall Rule for HTTP Traffic .................................267
Figure 71: Example of PPPoA on ADSL Interface .........................................267
Figure 72: Example of PPPoE on ADSL Interface with Backup .................269
Figure 73: Example of DIP Group Configuration .........................................274
Figure 74: Configure New Cluster ...............................................................274
Figure 75: Configure New Global DIP .........................................................276
Figure 76: Configure New Global DIP..........................................................277
Figure 77: Configure Firewall Rule to Use Global DIP Object ......................278
Figure 78: Configuring PPPoE Overview .....................................................280
Figure 79: Configure Ethernet1 DHCP Server Settings ...............................281
Figure 80: Configuring Multiple PPPoE Instances on an Interface ..............283
Figure 81: Configure Sub Interface for Los Angeles on Ethernet3 ..........284
Figure 82: Configuring DNS Proxies Example Overview .............................290
Figure 83: Configuring DDNS Example Overview ........................................293
Figure 84: Configuring DDNS Instance .......................................................294
Figure 85: NSGP Example Overview .........................................................346
Figure 86: NSGP Connection Dialog Box ...................................................348
Figure 87: Configure Firewall Rule for GTP Traffic ......................................348
Figure 88: Configure L2TP Local User ..........................................................349
Figure 89: 8G SPM Aggregate Interfaces .....................................................362
Figure 90: 8G2 SPM and the 5000M2 Management Module .......................362
Figure 91: Example Single Port L2V Configuration ....................................363
Figure 92: Example of NSRP Active/Passive Configuration .........................379
Figure 93: Configuring VSD Group Masters ................................................384
Figure 94: Delta Configuration Summary Example ....................................402
Figure 95: Delta Configuration Summary Example ....................................403
Figure 96: Job Manager Module .................................................................407
Figure 97: Job Information Dialog Box .......................................................408
Figure 98: Failed Update Job Dialog Box ....................................................410
Figure 99: Attack Update Summary ............................................................422
Figure 100: Import/Update Architecture .....................................................432
Figure 101: Data Model Update ..................................................................434
Figure 102: Data Model Importing ......................................................... 435
Figure 103: Attack Viewer .................................................................... 454
Figure 104: New Dynamic Group .......................................................... 476
Figure 105: New Dynamic Group Members ........................................... 477
Figure 106: Create New Custom URL List .............................................. 483
Figure 107: Changing Default Action for URL Category ................. 485
Figure 108: RADIUS Authentication Server Overview ..................... 501
Figure 109: Configure RADIUS Auth Server ......................................... 504
Figure 110: Configure Firewall Rule To Authenticate Accountant Access 511
Figure 111: Configure External User Groups for Sales and Marketing ... 514
Figure 112: Configure Group Expression for Sales and Marketing ....... 515
Figure 113: Configure Rule Options to Authenticate Sales and Marketing 515
Figure 114: Protected Resource Overview ........................................... 521
Figure 115: Set Individual Sources and Destinations in a Firewall Rule 538
Figure 116: Set Group Sources and Destinations in a Firewall Rule .... 539
Figure 117: Negate Source in a Firewall Rule ......................................... 539
Figure 118: Set Standard Services in a Firewall Rule ............................ 540
Figure 119: Set Custom Services in a Firewall Rule ............................. 540
Figure 120: Select WEB Filtering Rule Option in a Firewall Rule ......... 549
Figure 121: Configure WEB Filtering in a Firewall Rule ..................... 549
Figure 122: Configure Source/Destination for Multicast Rule ............. 555
Figure 123: Set Source and Destination ................................................ 558
Figure 124: Set Multiple Source and Destination Networks .............. 558
Figure 125: Set Default Services .......................................................... 559
Figure 126: Set Custom Services ........................................................... 559
Figure 127: Add Non-Standard Services Object ................................... 560
Figure 128: Set Non-Standard Service .................................................. 560
Figure 129: Set Terminal Rules .............................................................. 562
Figure 130: Firewall Rule for Dedicated IDP ......................................... 568
Figure 131: IDP Rules for Dedicated IDP .............................................. 568
Figure 132: Exempting Source and Destination ................................... 570
Figure 133: Exempting Attack Object .................................................. 571
Figure 134: Exempting a Log Record Rule .......................................... 572
Figure 135: View Rule Shadowing Example ......................................... 578
Figure 136: View Unsupported Feature Warning Message ................. 579
Figure 137: Install New Security Policies .............................................. 580
Figure 138: Zone Exceptions Example ................................................ 584
Figure 139: Zone Exceptions Example Rule .......................................... 584
Figure 140: Security Policy A Rules (Before Policy Merge) ............... 587
Figure 141: Security Policy B Rules (Before Policy Merge) ............... 588
Figure 142: Configure Policy Merge .................................................... 588
Figure 143: Security Policy Rules (Merged from Policy A and Policy B) 589
Figure 144: Export Policy Dialog with Options Selected .................... 590
Figure 145: Site-to-Site VPN Overview ................................................ 595
Figure 146: Hub and Spoke VPN Overview ......................................... 596
Figure 147: Full Mesh VPN Overview .................................................. 597
Figure 148: Configure AutoKey IKE VPN Example Overview ............. 628
Figure 149: Create Tokyo Protected Resource Object for AutoKey IKE VPN 630
Figure 150: Create Paris Protected Resource Object for AutoKey IKE VPN 630
Figure 151: Configure Gateway Parameters for AutoKey IKE VPN .... 632
Figure 152: View Autogenerated Rules for AutoKey IKE VPN ............ 632
Figure 153: AutoKey IKE RAS VPN Example Overview ..................... 633
Figure 154: Add Chicago Protected Resource for AutoKey IKE RAS VPN 634
Figure 155: Add New Local User for AutoKey IKE RAS VPN ............. 635
Figure 156: Configure Security for AutoKey IKE RAS VPN .......................... 636
Figure 157: View Autogenerated Rules for AutoKey IKE RAS VPN .......... 636
Figure 158: AutoKey IKE, RB Site-to-Site VPN Example Overview .......... 637
Figure 159: Configure Members for AutoKey IKE, RB Site-to-Site VPN ..... 639
Figure 160: View Members for AutoKey IKE, RB Site-to-Site VPN ........... 639
Figure 161: Configure Security for AutoKey IKE, RB Site-to-Site VPN ..... 640
Figure 162: View Tunnel Summary for AutoKey IKE, RB Site-to-Site VPN ... 640
Figure 163: Configure Untrust Route for AutoKey IKE, RB Site-to-Site VPN ... 641
Figure 164: Configure Trust Route for AutoKey IKE, RB Site-to-Site VPN ..... 642
Figure 165: View Routing Table for AutoKey IKE, RB Site-to-Site VPN .... 642
Figure 166: Configure Untrust Route for AutoKey IKE, RB Site-to-Site VPN ... 643
Figure 167: Configure Trust Route for AutoKey IKE, RB Site-to-Site VPN .... 643
Figure 168: View Routing Table for AutoKey IKE, RB Site-to-Site VPN ...... 644
Figure 169: Add New Protected Resource for FTP Server ....................... 647
Figure 170: Configure Remote User (Reseller Local User Group) ............. 648
Figure 171: Configure Security for Reseller VPN .................................. 649
Figure 172: View Autogenerated Rules for Reseller VPN ......................... 649
Figure 173: Configure IKE IDs/XAuth Overrides for Reseller VPN ............ 650
Figure 174: RB Site-to-Site VPN, MK Example Overview ....................... 666
Figure 175: Configure Tokyo Route for RB Site-to-Site VPN, MK ............ 668
Figure 176: Configure Tokyo Trust Route for RB Site-to-Site VPN, MK ...... 669
Figure 177: View Tokyo Routing Table for RB Site-to-Site VPN, MK ........ 669
Figure 178: Configure Paris Untrust Route for RB Site-to-Site VPN, MK .... 671
Figure 179: Configure Paris Trust Route for RB Site-to-Site VPN, MK ...... 671
Figure 180: Paris Routing Table for RB Site-to-Site VPN, MK ............... 672
Figure 181: Configure Rules for RB Site-to-Site VPN, MK ..................... 672
Figure 182: PB Site-to-Site VPN, MK Example Overview ......................... 673
Figure 183: Configure Two VPN Rules for PB Site-to-Site VPN, MK ........ 675
Figure 184: PB RAS VPN, L2TP Example Overview .................................. 676
Figure 185: Configure Rule for PB RAS VPN, L2TP ................................. 678
Figure 186: Device Monitor Dialog Box ................................................. 683
Figure 187: View Device Detail Status ..................................................... 687
Figure 188: Device Statistics Dialog Box ............................................... 688
Figure 189: Device Statistics Bar Graph ................................................. 691
Figure 190: Protocol Distribution Dialog Box ............................................ 693
Figure 191: Monitoring VPNs ................................................................. 707
Figure 192: Server Monitor ................................................................. 713
Figure 193: Viewing Device Server Details ............................................. 715
Figure 194: Process Status for the Device Server .................................... 716
Figure 195: Process Status for the GUI Server ....................................... 716
Figure 196: Log Viewer UI Overview ...................................................... 736
Figure 197: View Category and Severity Filters Messages ....................... 740
Figure 198: Log Viewer Navigation Controls ........................................... 740
Figure 199: Log Viewer Time Slider ..................................................... 742
Figure 200: Log Viewer Time Display .................................................... 742
Figure 201: Viewing Summary Panel ..................................................... 753
Figure 202: Log Investigator UI Overview .............................................. 755
Figure 203: Configure Time Period Filter .............................................. 757
Figure 204: Changing Time Period Filter ............................................... 757
Figure 205: View Log Investigator Results ............................................. 761
Figure 206: Audit Log Viewer UI Overview ............................................ 765
Figure 207: Create a Custom Report ..................................................... 787
Figure 208: Log Viewer Information for Top Information Logs Report ....... 794
Figure 209: Generating Quick Reports ................................................... 795
Figure 210: Select Log Viewer Flag ........................................................................ 796
Figure 211: Logs by User-Set Flag Reports .............................................................. 797
Figure 212: Top Rules Report Dialog Box .............................................................. 798
Figure 213: FW/VPN Report ................................................................................ 799
Figure 214: CIDR Translation .............................................................................. 806
List of Tables

Table 1: GUI Server Processes ................................................................. 13
Table 2: Device Server Processes ............................................................. 14
Table 3: Supported Security Devices ....................................................... 14
Table 4: Validation Status for Devices .................................................... 22
Table 5: Validation Icons ..................................................................... 22
Table 6: Predefined NetScreen-Security Manager Administrator Activities .. 60
Table 7: Security Device Port Mode Summary (Part 1) ............................ 85
Table 8: Security Device Port Mode Summary (Part 2) ............................ 86
Table 9: CSV File Information for Devices with Static IP Addresses ........ 121
Table 10: CSV File Information for Devices with Dynamic IP Addresses .... 122
Table 11: CSV File Information for Undeployed Devices ......................... 123
Table 12: Predefined DHCP Option Codes for DHCP Servers ................. 227
Table 13: Assigned IP Addresses for Office A and Office B .................... 239
Table 14: IP Addresses for VSIs ............................................................ 254
Table 15: Wireless Interface-to-Zone Mapping ....................................... 272
Table 16: Trickling Settings .................................................................. 319
Table 17: Delta Configuration Summary Information .............................. 400
Table 18: Device States During Update .................................................. 409
Table 19: Scheduled Security Update Post Actions ................................. 423
Table 20: Deep Inspection Profile Actions .............................................. 452
Table 21: Deep Inspection IP Actions ..................................................... 453
Table 22: IP Protocol Name and Type Numbers ..................................... 461
Table 23: Supported Services for Service Bindings ................................ 462
Table 24: Attack Pattern Syntax ............................................................ 464
Table 25: Attack Pattern Syntax Example Matches ................................. 465
Table 26: DI Attack Header Match Modifiers ........................................ 467
Table 27: Supported Protocols ............................................................... 470
Table 28: Service Table Tab Information ................................................. 492
Table 29: Group Expression Operators .................................................. 513
Table 30: IDP Rule Actions .................................................................. 562
Table 32: Actions for Backdoor Rule: ................................................... 575
Table 33: Device Status Information ....................................................... 683
Table 34: Device Polling Intervals .......................................................... 685
Table 35: Device Detail Status Items ....................................................... 687
Table 36: Device Statistics Summary Items ............................................. 689
Table 37: Device Specific Views ............................................................. 689
Table 38: Policy Distribution Items ....................................................... 691
Table 39: Protocol Distribution Items .................................................... 693
Table 40: VPN Monitor Table ................................................................. 695
Table 41: Active VPN Table ................................................................. 696
Table 42: Ethernet Statistics View Data ................................................. 698
Table 43: Flow Statistics View Data ....................................................... 699
Table 44: Attack Counters ................................................................. 699
Table 45: Resource Statistics Items ....................................................... 702
Table 46: Administrators View ............................................................. 703
Table 47: Authenticated Users View ..................................................... 703
Table 48: Active Sessions Items ............................................................ 703
Table 49: HA Statistics View ............................................................... 706
Table 50: VPN Tunnel Summary .......................................................... 707
Table 51: NSRP Device Summary................................................................. 709
Table 52: VSD/RTO Summary................................................................. 709
Table 53: VSD Counter Details............................................................... 710
Table 54: RTO Counters Details............................................................. 710
Table 55: Server Information................................................................. 712
Table 56: Server Monitor Data............................................................... 714
Table 57: Server Detail Status............................................................... 715
Table 58: Process Status................................................................. 717
Table 59: Event-Generated Log Entries.................................................... 721
Table 60: Log Categories ...................................................................... 721
Table 61: Log Entry Severties ................................................................. 722
Table 62: Destinations of Log Entry Severties ........................................ 725
Table 63: Self Log Entry Settings .......................................................... 726
Table 64: Email Server Settings for Log Entries ...................................... 726
Table 65: Syslog Settings for Log Entries ................................................ 734
Table 66: WebTrends Settings for Log Entries ......................................... 734
Table 67: Log Viewer Columns ............................................................... 736
Table 68: Search Tools for Log Viewer.................................................. 741
Table 69: Log Viewer Flags .................................................................. 743
Table 70: Irrelevant Vs. Relevant Attacks .................................................. 753
Table 71: Log Investigator Filters ........................................................ 760
Table 72: Log Investigator Analysis ....................................................... 762
Table 73: Audit Log Information ............................................................ 765
Table 74: Common Filters for Exporting Log Records ......................... 774
Table 75: Firewall and VPN Reports ..................................................... 784
Table 76: DI/IDP Reports .................................................................... 784
Table 77: Screen Reports ..................................................................... 785
Table 78: Administrative Reports ........................................................ 786
Table 79: Unmanaged Commands ....................................................... 823
Table 80: SurfControl URL Categories .................................................. 825
Table 81: Screen Alarm Log Entries...................................................... 832
Table 82: Alarm Log Entries ................................................................. 833
Table 83: Configuration Log Entries .................................................... 899
Table 84: Information Log Entries ....................................................... 900
Table 85: Basic GTP Log Entry .............................................................. 902
Table 86: Extended GTP Log Entry ..................................................... 902
Table 87: Deleted GTP Tunnel Log Entry ........................................... 902
List of Examples

<table>
<thead>
<tr>
<th>Example</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using a Naming Convention for Security Devices</td>
<td>49</td>
</tr>
<tr>
<td>Using a Naming Convention for Address Objects</td>
<td>49</td>
</tr>
<tr>
<td>Configuring Role-Based Administration</td>
<td>66</td>
</tr>
<tr>
<td>Configuring an IDP-Only Administrator</td>
<td>70</td>
</tr>
<tr>
<td>Adding a Vsys Cluster</td>
<td>116</td>
</tr>
<tr>
<td>Using an Excel File to Add Multiple Static IP Devices</td>
<td>121</td>
</tr>
<tr>
<td>Using a Text File to Add Multiple Static IP Devices</td>
<td>121</td>
</tr>
<tr>
<td>Using an Excel File to Add Multiple Dynamic IP Devices</td>
<td>122</td>
</tr>
<tr>
<td>Using a text File to Add Multiple Dynamic IP Devices</td>
<td>123</td>
</tr>
<tr>
<td>Using an Excel File to Add Multiple Modeled Devices</td>
<td>124</td>
</tr>
<tr>
<td>Using a text File to Add Multiple Modeled Devices</td>
<td>124</td>
</tr>
<tr>
<td>Creating a Device Template For DNS Settings</td>
<td>136</td>
</tr>
<tr>
<td>Applying a Device Template</td>
<td>137</td>
</tr>
<tr>
<td>Using Multiple Device Templates</td>
<td>143</td>
</tr>
<tr>
<td>Creating a Device Group</td>
<td>149</td>
</tr>
<tr>
<td>Creating an Access List on a virtual router</td>
<td>172</td>
</tr>
<tr>
<td>Configuring an Export Rule on a virtual router</td>
<td>175</td>
</tr>
<tr>
<td>Configuring Automatic Export on a virtual router</td>
<td>177</td>
</tr>
<tr>
<td>Using Source-Based Routing</td>
<td>181</td>
</tr>
<tr>
<td>Configuring Source Interface-Based Routing</td>
<td>183</td>
</tr>
<tr>
<td>Configuring OSPF</td>
<td>192</td>
</tr>
<tr>
<td>Configuring PIM</td>
<td>207</td>
</tr>
<tr>
<td>Configuring a Static Multicast Route Entry</td>
<td>211</td>
</tr>
<tr>
<td>Configuring UDP Flood Protection by Limiting UDP Packets</td>
<td>215</td>
</tr>
<tr>
<td>Blocking Malicious URLs in Packet Fragments</td>
<td>221</td>
</tr>
<tr>
<td>Configuring UDP Flood Protection by Limiting UDP Packets</td>
<td>222</td>
</tr>
<tr>
<td>Configuring Custom Options For a DHCP Server</td>
<td>228</td>
</tr>
<tr>
<td>Configuring a MIP on the Untrust Interface</td>
<td>231</td>
</tr>
<tr>
<td>Configuring a VIP</td>
<td>234</td>
</tr>
<tr>
<td>Creating a DIP Pool with Port Address Translation (PAT)</td>
<td>237</td>
</tr>
<tr>
<td>Using DIP in a Different Subnet</td>
<td>239</td>
</tr>
<tr>
<td>Configuring an Interface DIP For Sip</td>
<td>245</td>
</tr>
<tr>
<td>Configuring an Incoming DIP Pool for Sip</td>
<td>247</td>
</tr>
<tr>
<td>Configuring an Aggregate Interface</td>
<td>250</td>
</tr>
<tr>
<td>Configuring a Loopback Interface</td>
<td>252</td>
</tr>
<tr>
<td>Configuring Redundant Interfaces for VSI Groups</td>
<td>253</td>
</tr>
<tr>
<td>Configuring a Subinterface in the Root System</td>
<td>257</td>
</tr>
<tr>
<td>Configuring aDSL1 to Access to Local Servers</td>
<td>264</td>
</tr>
<tr>
<td>Configuring aDSL1 for PPPoA</td>
<td>267</td>
</tr>
<tr>
<td>Configuring aDSL1 for PPPoE with Backup (Modem Port)</td>
<td>269</td>
</tr>
<tr>
<td>Configuring a DIP Group on the device</td>
<td>273</td>
</tr>
<tr>
<td>configuring PPPoE and DHCP</td>
<td>280</td>
</tr>
<tr>
<td>Configuring Multiple PPPoE Instances on a Single Interface</td>
<td>283</td>
</tr>
<tr>
<td>Configuring DNS Proxies</td>
<td>290</td>
</tr>
</tbody>
</table>
Configuring Dynamic DNS (DDNS) ................................................................. 292
Configuring Permitted IPs ............................................................................ 302
Turning on Antispam in a Policy ................................................................. 321
Configuring Antispam in a template ............................................................. 321
Configuring integrated web filtering ............................................................ 323
Configuring Websense Redirect Web Filtering ............................................ 325
Configuring NSGP ....................................................................................... 346
Configuring an L2TP Local User ................................................................. 350
Using VLAN tags at Vsys Level ................................................................. 355
Using IP Classification ............................................................................... 357
Configuring a Single VLAN on a Single Port .............................................. 362
Configuring NSRP for an Active/Passive Configuration .............................. 378
Changing VSD Group Member State ........................................................... 384
Updating Devices With Different Attack Object Database Versions ............ 420
Confirm IDP Engine Version ....................................................................... 421
Using Cron Tab to Schedule Attack Updates .............................................. 425
CREATING A DYNAMIC GROUP ................................................................. 476
Configuring an External AV Profile ............................................................ 479
Creating a URL Custom list ....................................................................... 482
creating a Web Filtering Custom Profile ...................................................... 484
Viewing the predefined profile .................................................................... 485
Creating a GTP Object ............................................................................... 491
Creating a Custom Service and Group ....................................................... 495
Creating a Custom Sun-rpc Service ............................................................. 496
Creating a Custom MS-rpc Service .............................................................. 497
Configuring a RADIUS Auth Server ........................................................... 503
Using RADIUS with User Groups .............................................................. 509
Configuring an IP Pool Object .................................................................... 512
Creating a Group Expression ...................................................................... 514
Setting Individual Sources and Destinations in rules ................................. 538
Setting Group Sources and Destinations in rules ....................................... 539
Negating Sources in rules .......................................................................... 539
Setting Standard Services in rules .............................................................. 540
Setting Custom Services in rules ............................................................... 540
Setting Schedule Objects in rules .............................................................. 547
Setting a WEB Filtering Profile in a Rule ................................................. 548
Creating a Multicast Rule .......................................................................... 554
Setting Source and Destination ................................................................. 557
Setting Multiple Sources and Destinations ................................................. 558
Setting Default Services .......................................................................... 559
Setting Custom services ........................................................................... 559
Setting Non-Standard Services .................................................................. 559
Setting Terminal Rules .............................................................................. 561
Configuring Rules for a Standalone IDP System ......................................... 568
Exempting a Source/Destination Pair ......................................................... 570
Exempting Specific Attack Objects ............................................................ 571
Using Zone Exceptions ............................................................................... 583
Merging Security Policies .......................................................................... 587
Exporting Zone based Firewall rules with expanded view ............................ 589
Configuring an AutoKey IKE, Policy-Based Site-to-Site VPN ...................... 628
Configuring an AutoKey IKE RAS, Policy-Based VPN ............................... 633
Configuring an AutoKey IKE, Route-Based Site-to-Site VPN ...................... 637
Configuring XAuth Authentication with External User Group .................... 644
Configuring a Route-Based Site-to-Site VPN, Manual Key ......................... 665
Configuring a Policy-Based Site-to-Site VPN, Manual Key .............................673
Configuring a Policy-Based RAS VPN, L2TP.................................................676
Monitoring Device Status .............................................................................711
Tailing incoming Logs in the Log Viewer......................................................743
Using Filters in the log Viewer..................................................................747
Customizing Log Viewer Columns...............................................................749
Setting a Time Interval in the Log Investigator ..........................................757
Using Left and Top Axes in the Log Investigator........................................758
Setting Filters in the Log Investigator ..........................................................760
Viewing Destination Ports in the Log Investigator .....................................763
Viewing Subcategory Details in the Log Investigator .................................763
Viewing Time Period in the log investigator ...............................................763
Exporting Attack Category Log Records to XML......................................775
Exporting Column Headers to CSV............................................................776
Exporting to a SNMP Server......................................................................777
Using Administrative Reports to Track Incidents......................................795
Using Administrative Reports to Optimize Rulebases...............................797
Using FW/VPN Report to Track Configuration Changes............................798
Using Screen Reports to Identify Attack Trends .......................................799
Using DI Reports to Detect Application Attacks.......................................799
About This Guide

Juniper Networks NetScreen-Security Manager 2005.3 is a software application that centralizes control and management of your Juniper Networks security devices. With NetScreen-Security Manager, Juniper Networks delivers integrated, policy-based security and network management for all security devices.

NetScreen-Security Manager uses the technology developed for Juniper Networks ScreenOS to enable and simplify management support for previous and future versions of ScreenOS. By integrating management of all Juniper Networks security devices, NetScreen-Security Manager enhances the overall security of the Internet gateway.

This Administrator’s Guide describes NetScreen-Security Manager features and provides a technical overview of the management system architecture. It also explains how to configure basic and advanced NetScreen-Security Manager functionality, including adding new devices, deploying new device configurations, updating device firmware, managing Security Policies and VPNs, viewing log information, and monitoring the status of your network. Use this guide in conjunction with the NetScreen-Security Manager Online Help, which provides step-by-step instructions for many of the processes described in this document.

NOTE: If the information in the latest NetScreen-Security Manager 2005.3 Release Notes differs from the information in this guide, follow the NetScreen-Security Manager 2005.3 Release Notes.

The following sections are in this chapter:

- Audience
- Conventions
- Documentation
- Contacting Customer Support
Audience

This guide is intended for system administrators that are responsible for the security infrastructure of their organization. Specifically, this book discusses concepts of interest to firewall and VPN administrators, network/security operations center administrators; and system administrators responsible for user permissions on the network.

Conventions

This document uses the conventions detailed in the following sections.

User Interface Conventions

The sample screens used in this guide are representations of the screens displayed in the NetScreen-Security Manager UI. Throughout this book, a chevron ( > ) indicates navigation in the UI by clicking menu options and links. For example, to view the Paris device configuration, the path is presented as **Device Manager > Security Devices > Paris**, as shown below.

Figure 1: UI Navigation Example

1. In the main navigation tree, double-click Device Manager. The Device Manager tree expands.

2. In the Device Manager navigation tree, select Security Device. The main display area displays all defined security devices.

3. In the Security Devices navigation tree, select the Paris security device.
Illustration Conventions

The following graphics make up the basic set of images used in illustrations throughout this book.

Figure 2: Graphic Conventions

Unsupported Characters

The following characters are not supported in the NetScreen-Security Manager UI:

- Control Characters (\(\leq 0x1F\))
- Unicode (\(\geq 0x100\))
- Quotation Mark (‘‘)
- Percent Sign (‘%’)
- Backslash (‘\’)
- Ampersand (‘&’) cannot be used as the first character in a field

NOTE: However, NetScreen-Security Manager does support the above characters in the Search Mode fields and the Attack Object editor.
Additionally, the following characters are not supported for NetScreen-Security Manager administrator names:

- Dot character ( . )
- Number sign ( # )
- Dollar sign ( $ )
- Asterisk ( * )
- Ampersand ( & )
- Circumflex ( ^ )

Documentation

This guide describes how to use and configure key management features in the NetScreen-Security Manager. It provides conceptual information, suggested workflows, and examples where applicable. This guide is best used in conjunction with the NetScreen-Security Manager Online Help, which provides step-by-step instructions for performing management tasks in the NetScreen-Security Manager UI.

This guide is intended for application administrators or those individuals responsible for the server and security infrastructure and configuring the product for multi-user systems. It is also intended for device configuration administrators, firewall and VPN administrators, and network security operation center administrators.

NetScreen-Security Manager 2005.3 Administrator’s Guide

The following sections detail each chapter in the NetScreen-Security Manager Administrator’s Guide.

Part 1: Preparing

Chapter 1 “Introduction to NetScreen-Security Manager” details NetScreen-Security Manager features and provides a technical overview of the system and its architecture. This chapter also includes a User Interface (UI) overview to help you get acquainted with the NetScreen-Security Manager UI.

Chapter 2 “Getting Started” provides a quick overview of supported security devices, including the IDP-capable security device, the ISG 2000 and ISG 1000 running ScreenOS 5.0.0-IDP1x. This chapter also provides guidance for using a naming convention for better object management, and some NetScreen-Security Manager-specific tools for handling multiple devices, objects, and policies.

Chapter 3 “Configuring Role-Based Administration” details the process of creating a domain structure, designing permissions, and preparing to add devices, objects, and policies.
Part 2: Integrating

Chapter 4 “Adding Devices” details how to add security devices to NetScreen-Security Manager. This chapter also describes how to use Rapid Deployment (RD) to quickly deploy devices in non-technical environments.

Chapter 5 “Configuring Devices” details how to create a device configuration, including zones, interfaces, and routes. This chapter also describes how to use templates and groups to manage multiple devices more efficiently.

Chapter 6 “Updating Devices” details how to use configuration summaries, update your device configurations, and use Job Manager to track the update progress.

Chapter 7 “Managing Devices” details how to maintain device features, manage device images, and update AntiVirus and Deep Inspection files on the device.

Part 3: Managing

Chapter 8 “Configuring Objects” details how to configure shared objects, such as address, service, schedule, attack objects, and NAT objects such as VIPs, MIPs, and DIPs.


Chapter 10 “Configuring VPNs” details how to create VPN components such as protected resources and IKE proposals, and guides you through building VPNs at the system level and at the device level.

Part 4: Monitoring

Chapter 11 “Monitoring” details the firewall, VPN, and NSRP monitoring functionality of NetScreen-Security Manager.

Chapter 12 “Logging” details how to manage, filter, and export firewall logs in the Log Viewer, how to investigate suspicious activity in the Log Investigator, and how to track administrative changes in the Audit Log Viewer.

Chapter 13 “Reporting” details how to create reports from log information.

Part 5: Appendixes

Appendix A, Glossary defines terms and concepts used in the NetScreen-Security Manager environment.

Appendix B, Unmanaged Commands details unsupported ScreenOS CLI commands.

Appendix C, SurfControl URL Categories details the predefined URL categories provided and maintained by SurfControl.

Appendix D, Log Entries details log entry categories and subcategories.

Appendix E, Common Criteria EAL2 Compliance details EAL2 common criteria for IDP-capable security devices.
Part 6: Index
The index provides an alphabetical list of the major topics and subtopics discussed in this document, and their corresponding page numbers.

Related Documentation
The NetScreen-Security Manager documentation includes the following guides:

NetScreen-Security Manager 2005.3 Installer’s Guide
This guide details the steps to install the NetScreen-Security Manager management system on a single server or on separate servers. It also includes information on how to install and run the NetScreen-Security Manager user interface. This guide is intended for IT administrators responsible for the installation and/or upgrade to NetScreen-Security Manager 2005.3.

NetScreen-Security Manager 2005.3 Online Help
The online help provides task-oriented procedures that describe how to perform basic tasks in the NetScreen-Security Manager user interface. It also includes a brief overview of the NetScreen-Security Manager system and a description of the GUI elements.

The online help is best used in conjunction with the NetScreen-Security Manager Administrator’s Guide, which provides conceptual information, suggested workflows, and examples for management tasks where applicable.

The online help is intended for network and security administrators who are using the UI to configure and manage devices.

NetScreen-Security Manager 2005.3 Release Notes
The release notes provide latest information about features, changes, known problems, resolved problems, and system maximum values. If the information in the Release Notes differs from the information found in the documentation set, follow the Release Notes.

Release notes are included on the corresponding software CD and are available on the Web.

Web Access
To obtain technical documentation for any Juniper Networks security product, visit www.juniper.net/techpubs/.

Comments About the Documentation
We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation to better meet your needs. Please e-mail your comments to:

- techpubs-comments@juniper.net

Along with your comments, be sure to indicate:
Contacting Customer Support

For technical support, contact Juniper Networks at support@juniper.net, or at 1-888-314-JTAC (within the United States) or 408-745-9500 (from outside the United States).
Part 1
Preparing

The chapters in Part 1 of the NetScreen-Security Manager 2005.3 Administrators Guide provide an overview of the management system and how to prepare to integrate your existing network security structure using NetScreen-Security Manager role-based administration tools.

Part 1 contains the following chapters:

- Chapter 1 “Introduction to NetScreen-Security Manager” details NetScreen-Security Manager features and provides a technical overview of the system and its architecture. This chapter also includes a User Interface (UI) overview to help you get acquainted with the NetScreen-Security Manager UI.

- Chapter 2 “Getting Started” provides a quick overview of supported security devices, including the IDP-capable security devices, the ISG 2000 and ISG 1000 running ScreenOS 5.0.0-IDP1x. This chapter also provides guidance for using a naming convention for better object management, and some NetScreen-Security Manager-specific tools for handling multiple devices, objects, and policies.

- Chapter 3 “Configuring Role-Based Administration” details the process of creating a domain structure, designing permissions, and preparing to add devices, objects, and policies.

After you have become familiar with NetScreen-Security Manager features and the UI, and you have designed a domain structure and administrator roles that meet the architectural and security needs of your network (or networks), you are ready to begin the process of integration, as detailed in Part 2, “Integrating” on page 71.
Chapter 1
Introduction to NetScreen-Security Manager

Juniper Networks NetScreen-Security Manager gives you complete control over your network. Using NetScreen-Security Manager, you can configure all your Juniper Networks security devices from one location, at one time. NetScreen-Security.

The following sections are in this chapter:

- About NetScreen-Security Manager 2005.3
- Technical Overview
- Working in the User Interface
- New Features for NetScreen-Security Manager 2005.3
About NetScreen-Security Manager 2005.3

At its foundation, a management system integrates your individual security devices into a single, effective security system that you control from a central location. With NetScreen-Security Manager, you can manage your network at the system level, using policy-based central management, as well as at the device level, managing all device parameters for devices.

NetScreen-Security Manager is designed to work with networks of all sizes and complexity. You can add a single device, or create device templates to help you deploy multiple devices; you can create new policies, or edit existing policies for security devices. The management system tracks and logs each administrative change in real-time, providing you with a complete administrative record and helping you perform fault management.

NetScreen-Security Manager also simplifies control of your network with an intuitive UI. Making all changes to your devices from a single, easy-to-use interface can reduce deployment costs, simplify network complexity, speed configuration, and minimize troubleshooting time.

The following sections detail the key management features of NetScreen-Security Manager.

Security Integration

True security integration occurs when you can control every security device on your network and see every security event in real-time from one location. In NetScreen-Security Manager, this location is the NetScreen-Security Manager UI, a graphical user interface that contains a virtual representation of every security device on your network. The idea behind this virtual-physical abstraction is that you can access your entire network from one location—use this console to view your network, the devices running on it, the policies controlling access to it, and the traffic that is flowing through it.

Complete Support

You can create and manage device configurations for security devices or systems. NetScreen-Security Manager provides support for ScreenOS configuration commands, so you can retain complete control over your devices when using system-level management features like VPNs.

Network Organization

Divide and conquer with NetScreen-Security Manager—use domains to segment your network functionally or geographically to define specific network areas that multiple administrators can manage easily.

A domain logically groups devices, their policies, and their access privileges. Use a single domain for small networks with a few security administrators, or use multiple domains for enterprise networks to separate large, geographically distant or functionally distinct systems, control administrative access to individual systems, or obfuscate systems for service provider deployments.
With multiple domains, you can create objects, policies, and templates in the global domain, then create subdomains that automatically inherit these definitions from the global domain.

**Role-Based Administration**

Control access to management with NetScreen-Security Manager—define strategic roles for your administrators, delegate management tasks, and enhance existing permission structures with new task-based functionality.

Use NetScreen-Security Manager to create a security environment that reflects your current offline administrator roles and responsibilities. Because management is centralized, it's easy to configure multiple administrators for multiple domains. By specifying the exact tasks your NetScreen-Security Manager administrators can perform within a domain, you minimize the probability of errors and security violations, and enable a clear audit trail for every management event.

Initially, when you log in to NetScreen-Security Manager as the super administrator, you have full access to all functionality within the global domain. From the global domain, you can add NetScreen-Security Manager administrators, configure their roles, and specify the subdomains to which they have access:

- **Activities and Roles**—An activity is a predefined task performed in the NetScreen-Security Manager system, and a role is a collection of activities that define an administrative function. Use activities to create custom roles for your NetScreen-Security Manager administrators.

- **Administrators**—An administrator is a user of NetScreen-Security Manager; each administrator has a specific level of permissions. Create multiple administrators with specific roles to control access to the devices in each domain.

- **Default Roles**—Use the predefined roles System Administrator, Read-Only System Administrator, Domain Administrator, and Read-Only Domain Administrator to quickly create permissions for your administrators.

**Centralized Device Configuration**

No network too large—because you manage your security devices from one location, you can use several system management mechanisms to help you quickly and efficiently create or modify multiple device configurations at one time:

- **Templates**—A template is simply a predefined device configuration that helps you re-use specific information. Create a device template that defines specific configuration values, then apply that template to devices to quickly configure multiple devices at one time. For more flexibility, you can combine and apply multiple device templates to a single device configuration. (63 maximum).

- **Shared Objects**—An object is a NetScreen-Security Manager definition that is valid in the global domain and all subdomains. Any object created in the global domain is a shared object that is shared by all subdomains; the subdomain automatically inherits any shared objects defined in the global domain.
The global domain is a good location for security devices and systems that are used throughout your organization, address book entries for commonly used network components, or other frequently used objects. A subdomain, alternatively, enables you to separate firewalls, systems, and address objects from the global domain and other subdomains, creating a private area to which you can restrict access.

- **Grouping**—A group is a collection of similar devices or objects. Use device groups and object groups to update multiple devices simultaneously, simplify rule creation and deployment, and enable group-specific reporting. You can even link groups using Group Expressions to create a custom group.

**Migration Tools**

If you have existing security devices deployed on your network or are using a previous Juniper Networks management system, you can use the NetScreen-Security Manager migration tools to quickly import your existing security devices and their configurations, address books, service objects, policies, VPNs, and administrator privileges. As NetScreen-Security Manager imports your existing device configurations, it automatically creates your virtual network based on the configuration information.

You can import device configurations directly from your security device, or from your Juniper Networks Global PRO or Global PRO Express system. Import all your security devices at one time, or, if your network is large, import one domain at a time. When importing from Global PRO or Global PRO Express, NetScreen-Security Manager automatically transfers your existing domain structure.

For details on migrating from a previous management system, see the NetScreen-Security Manager Migration Guide.

**Device Management**

A production network is a living entity, constantly evolving to adapt to the needs of your organization. As your network grows, you might need to add new devices, reconfigure existing devices, update software versions on older devices, or integrate a new network to work with your existing network. NetScreen-Security Manager helps you take control of your network by providing a virtual environment in which to first model, verify, then updated your managed devices with changes.

**Device Modeling**

Using your virtual network to change, review, and test your network configuration before deploying it to your physical network can help you discover problems like routing issues, IP conflicts, and version mismatches across your entire network before they actually occur. NetScreen-Security Manager includes configuration validation to help you identify device configuration errors and missing information, then points you to the trouble spot so you can quickly fix the problem. When you have designed a virtual configuration that works, you can push this configuration to your devices with a single update.
With NetScreen-Security Manager, you can implement a new routing protocol across your network, design and deploy a new Security Policy with traffic shaping, or create a new VPN tunnel that connects a branch office to your corporate network—then deploy all changes with a single click.

Rapid Deployment (RD)
Rapid Deployment (RD) enables deployment of multiple security devices in a large networked environment with minimal user involvement. RD is designed to simplify the staging and configuration of security devices in non-technical environments, enabling the secure and efficient deployment of a large number of devices.

To use RD, the NetScreen-Security Manager administrator creates a small file (called a configlet) in NetScreen-Security Manager, then sends that configlet to an on-site administrator that has local access to the security device. With the help of the Rapid Deployment wizard, the on-site administrator installs the configlet on the device, which automatically contacts NetScreen-Security Manager and establishes a secure connection for device management.

RD is ideal for quickly bringing new security devices under NetScreen-Security Manager management for initial configuration. You can model and verify your device configurations for undeployed devices, then install the completed device configuration when the device contacts NetScreen-Security Manager.

Policy-Based Management
Create simplified and efficient Security Policies for your managed devices using:

- **Groups**—Group your devices by platform, ScreenOS version, location, or function, then add them to your Security Policies.

- **Zone Exceptions**—To simplify your rules, define a common To Zone and From Zone for all devices in the rule, then specify zone exceptions to change the To and From zones for specific devices. Zone exceptions add flexibility to your firewall rules, enabling you to manage more devices in a single rule.

- **Filtering**—Filter on From and To Zones to see rules between zones.

- **Scheduling**—Schedule a time or time period that a rule in your Security Policy is in effect on the devices in a rule. Create schedule objects as one-time, recurring, or both; you can even select multiple schedule objects in a firewall rule.

- **Security and Protection**—Configure a rule to look for attacks, viruses, or specific URLs (devices running ScreenOS 5.x only).

- **Traffic Shaping**—Use your firewall rules to control the amount of traffic permitted through your security devices.

**Error Prevention, Recovery, and Auditing**
Persistent management control is essential when managing large networks. You need to be sure that configuration and policies you send to your managed devices are correct before you install them on your devices.
Using NetScreen-Security Manager’s error prevention and recovery features, you can ensure that you are consistently sending stable configurations to your devices, and that your device remain connected to NetScreen-Security Manager. Additionally, you can track each change made by an NetScreen-Security Manager administrator to help you identify when, how, and what changes were made to your managed devices.

Device Configuration Validation
NetScreen-Security Manager automatically alerts you to configuration errors while you work in the UI. Each field that has incorrect or incomplete data displays a icon—simply move your mouse cursor over the icon to get details on the missing data. For more details on validation, see “Validation Icons in the User Interface” on page 22.

Policy Validation
The policy validation tool checks your Security Policies and alerts you to possible problems before you install that policy on your managed devices.

Atomic Configuration and Updating
On devices running ScreenOS 5.x, if the configuration deployment fails for any reason, the device automatically uses the last installed stable configuration. Additionally, if the configuration deployment succeeds, but the device loses connectivity to the management system, the device restores the last installed configuration. This minimizes downtime and ensures that NetScreen-Security Manager always maintains a stable connection to the managed device.

Devices running ScreenOS 5.1 and higher also support atomic updating, which enables the device to receive the entire modeled configuration (all commands) before executing those commands (instead of executing commands as they are received from the management system). Because the device no longer needs to maintain a constant connection to the management system during updating, you can configure changes to management connection from the NetScreen-Security Manager UI.

Device Image Updates
You can update the software that runs on your devices by installing a new ScreenOS image on all your security devices:

- **NetScreen-Security Manager updates**—Use NetScreen-Security Manager to upload the new image file to multiple security devices with a single click.

- **RMA updates**—To replace failed devices, simply set the device to the RMA state, which enables NetScreen-Security Manager to retain the device configuration without a serial number or connection statistics. When you install the replacement device, just activate the device with the serial number of the replacement unit.
Auditing

Use the Audit Log Viewer to track administrative actions so you’ll always know exactly when and what changes were made using the management system. The Audit Log Viewer displays log entries in the order generated, and includes:

- Date and time the administrative action occurred
- NetScreen-Security Manager administrator who performed the action
- Action performed
- Domain (global or a subdomain) in which the action occurred
- Object type and name

The detail view of the Audit Log Viewer displays changes from the previous version.

Complete System Management

NetScreen-Security Manager provides the tools and features you need to manage your devices as a complete system, as well as individual networks and devices:

- To manage an individual device, create a single device configuration, define a Security Policy for that device, and monitor the device status.
- To manage a network, create multiple device configurations, define and install policies for multiple devices, and view the status of all devices in the same UI.
- To manage at the system level, create templates and use them to quickly configure multiple policies and VPNs that control the flow of traffic through your network, view system-wide log information for network security events, and monitor the status of NSRP.

VPN Abstraction

Use VPN Manager to design a system level VPN and automatically set up all connections, tunnels, and rules for all devices in the VPN. Instead of configuring each device as a VPN member and then creating the VPN, start from a system perspective: Determine which users and networks need access to each other, then add those components to the VPN.

Using AutoKey IKE, you can create the following VPNs with VPN Manager:

- Dynamic, route-based VPNs—Provide resilient, always-on access across your network. Add firewall rules on top of a route-based VPN to control traffic flow.
- Policy-based VPNs—Connect devices, remote access service (RAS) users, and control traffic flow (can also create with L2TP).
- Mixed-mode VPNs—Connect route-based VPNs with policy-based VPNs, giving you flexibility.
Integrated Logging and Reporting
You use the security devices on your network for multiple reasons: to control access to and from your network, to detect and prevent unwanted intruders, and to record security events so you can monitor the important activities occurring on your network. You can use NetScreen-Security Manager to monitor, log, and report on network activity in real-time to help you understand what is happening on your network:

- View traffic log entries generated by network traffic events, configuration log entries generated by administrative changes, or create custom views to see specific information in the Log Viewer.
- Create detailed reports from traffic log information in the Report Manager.
- Inspect suspicious events by correlating log information in the Log Investigator.

Monitoring Status
NetScreen-Security Manager keeps you up-to-date on the health of your network.

- View critical information about your device in the Device Monitor:
  - Configuration and connection status of your security devices
  - Individual device details, such as memory usage and active sessions
  - Device statistics
- View the status of each individual VPN tunnel in the VPN Monitor.
- View NSRP status in the NSRP Monitor.
- View the health of the NetScreen-Security Manager system itself, including CPU utilization, memory usage, and swap status in the Server Monitor.

Job Management
You can view the progress of communication to and from your devices in the Job Manager. NetScreen-Security Manager sends commands to managed devices at your request, typically to import, update or reboot devices, and view configuration and delta configuration summaries. When you send a command to a device or group of devices, NetScreen-Security Manager creates a job for that command and displays information about that job in the Job Manager module.

Job Manager tracks the progress of the command as it travels to the device and back to the management system. Each job contains:

- Name of the command
- Date and time the command was sent
- Completion status for each device that received the command
- Detailed description of command progress
Command output, such as a configuration list or CLI changes on the device

NOTE: Job Manager configuration summaries and job information details do not display passwords in the list of CLI commands for administrators that do not have the assigned activity "View Device Passwords". By default, only the super administrator has this assigned activity.

Technical Overview

Security from bottom up—NetScreen-Security Manager architecture is built on a secure foundation, with secure communication between management components and a single access point for inbound connections.

NOTE: For details on NetScreen-Security Manager architecture and help with setting up the management system, see the NetScreen-Security Manager Installer's Guide.

Architecture

NetScreen-Security Manager is a three tier management system comprised of a User Interface, management system, and managed devices (security devices). These three tiers combine to manage your security devices, which process your network traffic and are the enforcement points that implement your policies. The UI and management system tiers are software, not hardware, so you can deploy them quickly and easily. Additionally, because the management system uses internal databases for storage and authentication, you do not need LDAP or an external database.

Figure 1: NetScreen-Security Manager Network Architecture
UI

The UI is software that provides a powerful, graphical environment for centrally managing your network. The UI is a software application that can be installed on multiple computers on your network. You use the UI to remotely access the management system.

Multiple NetScreen-Security Manager admins can interact with security devices using the UI, and can even configure unique UI preferences. The NetScreen-Security Manager GUI Server stores user preferences in the central database so that they remain consistent when you access them from different client machines. The UI also provides extensive online help to help you use NetScreen-Security Manager quickly and efficiently.

The UI communicates with the GUI Server using a secure, proprietary, TCP-based connection that encrypts and authenticates all traffic.

Management System

The management system used in NetScreen-Security Manager provides all the functionality required to integrate management of all the components in your network security environment. It enables you to centrally gather, store, configure, manage, monitor and generate reports on the security devices you have deployed in your network.

The management system itself is composed of two distinct components:

- **GUI Server**
- **Device Server**

Both the GUI Server and Device Server working together are collectively referred to as the NetScreen-Security Manager “management system”.

Figure 2: NetScreen-Security Manager System Architecture
GUI Server

The GUI Server manages the system resources and data that drive NetScreen-Security Manager functionality. You can install the GUI Server software on a separate server, or on a Global PRO appliance. The GUI Server contains the NetScreen-Security Manager databases, and centralizes information for devices, their configurations, attack and server objects, and policies.

Specifically, the GUI Server stores all of the following information:

- Device, Security Policy, and VPN configuration
- NetScreen-Security Manager administrator accounts, device administrator accounts, and domains
- Objects
- Organizes and presents log entries from security devices (logs are stored on the Device Server)

The GUI Server receives logs from the Device Server on a single inbound port. When you use the UI to access NetScreen-Security Manager functionality, you connect using the same single port and access the databases stored on the GUI Server. The GUI Server communicates with the Device Server using SSP, a secure, proprietary, TCP-based connection that encrypts and authenticates all traffic.

When you start the GUI Server, it runs the following processes.

Table 1: GUI Server Processes

<table>
<thead>
<tr>
<th>Process</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>guiSvrManager</td>
<td>GUI Server Manager receives and responds to requests from the NetScreen-Security Manager User Interface. The GUI Server Manager forwards requests to the GUI Directive Handler or Device Directive Handler depending on the type of request for further processing.</td>
</tr>
<tr>
<td>guiSvrDirectiveHandler</td>
<td>GUI Directive Handler handles all directives or instructions from the NetScreen-Security Manager UI which require reading, writing or modifying of the local data store.</td>
</tr>
<tr>
<td>guiSvrStatus Monitor</td>
<td>GUI Server Status Monitor monitors the status of the processes that run on the GUI Server.</td>
</tr>
<tr>
<td>guiSvrMasterController</td>
<td>Master Controller forwards configuration data to the NetScreen-Security Manager UI (for viewing) or to the local data store (for later retrieval).</td>
</tr>
</tbody>
</table>

Device Server

The Device Server handles communication between the GUI Server and the device, collects data from the managed devices on your network, formats configuration information sent to your managed device, and consolidates log and event data.
You can install the GUI Server and the Device Server on the same physical computer, or separate computers. Communication between a physically separate GUI Server and the Device Server is an encrypted TCP connection to a default port. The Device Server connects to the GUI Server using the default port; you can change the default port by editing the configuration files for both servers.

If the GUI Server computer and the Device Server computer have a firewall between them, you must configure a rule on that firewall to permit NetScreen-Security Manager management traffic.

When you start the Device Server, it runs the following processes:

Table 2: Device Server Processes

<table>
<thead>
<tr>
<th>Process</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>devSvrManager</td>
<td>Device Server Manager enables security devices to connect to and communicate with the NetScreen-Security Manager management system. The Device Server Manager is writes log data into the local data store, and routes messages and directives from the GUI Server to the Device Directive Handler for further processing.</td>
</tr>
<tr>
<td>deviceDirectiveHandler</td>
<td>Device Directive Handler manages directives that are issued specifically to the security device (for example, a reboot, update firmware, or generate Config Summary command).</td>
</tr>
<tr>
<td>devSvrStatusMonitor</td>
<td>Device Server Status Monitor monitors the status of the processes that run on the Device Server.</td>
</tr>
<tr>
<td>devSvrDataCollector</td>
<td>Device Server Data Collector collects log data and device statistics from each security device managed by NetScreen-Security Manager.</td>
</tr>
<tr>
<td>devSvrLogWalker</td>
<td>Device Server Log Walker performs user-specified actions on log entries (such as indexing, de-duplication, filtering).</td>
</tr>
</tbody>
</table>

Managed Device

Managed devices are the security devices and systems that you use to enable access to your network components and to protect your network against malicious traffic.

The following table details the security devices and versions of ScreenOS supported by NetScreen-Security Manager:

Table 3: Supported Security Devices

<table>
<thead>
<tr>
<th>Security Device</th>
<th>ScreenOS Versions Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>Juniper Networks NetScreen-5XP</td>
<td>4.0.0, 4.0.1, 4.0.3, 5.0, 5.0 FIPS</td>
</tr>
<tr>
<td>Juniper Networks NetScreen-5XT</td>
<td>4.0.0, 4.0.1, 4.0.1MCAST, 4.0.3, 5.0, 5.1, 5.2, 5.3</td>
</tr>
<tr>
<td>Juniper Networks NetScreen-5GT</td>
<td>4.0.0-DIAL2, 5.0, 5.0DIAL, 5.0FIPS, 5.1, 5.2, 5.3</td>
</tr>
<tr>
<td>Juniper Networks NetScreen-5GT ADSL</td>
<td>5.0ADSL, 5.2, 5.3</td>
</tr>
<tr>
<td>Juniper Networks NetScreen-5GT WLAN</td>
<td>5.0WLAN, 5.3</td>
</tr>
<tr>
<td>Juniper Networks NetScreen-HSC</td>
<td>5.0, 5.0FIPS, 5.1, 5.2, 5.3</td>
</tr>
<tr>
<td>Juniper Networks NetScreen-25</td>
<td>4.0.0, 4.0.1, 4.0.1MCAST, 4.0.3, 5.0, 5.0FIPS, 5.1, 5.2, 5.3</td>
</tr>
</tbody>
</table>
Distributed Data Collection

The distributed data collection system provides NetScreen-Security Manager with a robust yet lightweight method for managing multiple objects. In NetScreen-Security Manager, each device is described by a unique Data Model (DM) that contains all the configuration data for that individual device. The Abstract Data Model (ADM) contains configuration data for all objects in a specific domain. When you use the UI to interface with your managed devices, the ADM and DMs work together:

- When you update a device configuration, the GUI Server translates the objects and object attributes in the ADM domain into device configuration information in a DM. The Device Server then translates the device configuration information in the DM into CLI commands and sends the commands to the device.

- When you import a device configuration, the device sends CLI commands to the Device Server, which translates the CLI commands into a DM with device configuration information. The GUI Server then translates the device configuration in the DM into objects and object attributes in the ADM, and uses the ADM to display current information in the UI.

The structure of the ADM and the DMs is defined by a DM schema, which lists all the possible fields and attributes for that type of object or device. The DM schema reads from a capability file, which lists the fields and attributes that a specific ScreenOS version supports, to determine the supported features for the ScreenOS version that is running on the managed devices. NetScreen-Security Manager uses capability files to enable Juniper Networks software upgrades without changing the device configuration in NetScreen-Security Manager.

For more details on the ADM and DMs, see Chapter 7, “Managing Devices”.

<table>
<thead>
<tr>
<th>Security Device</th>
<th>ScreenOS Versions Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>Juniper Networks NetScreen-50</td>
<td>4.0.0, 4.0.1, 4.0.1GMP, 4.0.1MCAST, 4.0.3, 5.0, 5.0FIPS, 5.1, 5.2, 5.3</td>
</tr>
<tr>
<td>Juniper Networks NetScreen-100</td>
<td>4.0.0</td>
</tr>
<tr>
<td>Juniper Networks NetScreen-204</td>
<td>4.0.0, 4.0.1, 4.0.1MCAST, 4.0.3, 5.0, 5.0FIPS, 5.1, 5.2, 5.3</td>
</tr>
<tr>
<td>Juniper Networks NetScreen-208</td>
<td>4.0.0, 4.0.1, 4.0.1MCAST, 4.0.3, 5.0, 5.0FIPS, 5.1, 5.2, 5.3</td>
</tr>
<tr>
<td>Juniper Networks NetScreen-500</td>
<td>4.0.0, 4.0.1, 4.0.1MCAST, 4.0.3, 5.0, 5.0FIPS, 5.0NSGP, 5.0GPRS, 5.1, 5.2, 5.3</td>
</tr>
<tr>
<td>Juniper Networks NetScreen-5200/8</td>
<td>4.0.0, 4.0.1, 4.0.1GMP, 4.0.1MCAST, 4.0.1SBR, 4.0.1SIBR, 4.0.3, 5.0, 5.0FIPS, 5.0NSGP, 5.0L2V, 5.1, 5.2, 5.3</td>
</tr>
<tr>
<td>Juniper Networks NetScreen-5400</td>
<td>4.0.1-SBR, 4.0.1-SIBR, 5.0, 5.0NSGP, 5.1, 5.3, 5.3</td>
</tr>
<tr>
<td>Juniper Networks ISG-1000</td>
<td>5.0, 5.0IDP1, 5.3</td>
</tr>
<tr>
<td>Juniper Networks ISG-2000</td>
<td>5.0, 5.0FIPS, 5.0IDP1, 5.2, 5.3</td>
</tr>
</tbody>
</table>
Security

NetScreen-Security Manager integrates application-level encryption and authentication and uses high-grade encryption and public-key algorithms to eliminate the need for separate IPSEC tunnels between each device and the management station.

For communication between the UI, the GUI Server, and the Device Server, NetScreen-Security Manager uses Secure Server Protocol (SSP), a modified version of TCP that is more reliable than ordinary TCP, requires less CPU and memory resources from servers, and reduces the number of acknowledgement packets on the network. SSP uses AES encryption and SHA1 authentication for all connections.

Scaling and Performance

NetScreen-Security Manager is designed to grow with your network, so you can continue to manage all your Juniper Networks network devices with NetScreen-Security Manager. As you add devices or network components to your physical network, you also add them to your virtual NetScreen-Security Manager network, where you can manage all future configurations. A NetScreen-Security Manager Device Server can support up to 1000 devices; the management system supports up to 30,000 log entries per second.

Working in the User Interface

The NetScreen-Security Manager User Interface (UI) is used to control the NetScreen-Security Manager system. Using the UI, you can configure NetScreen-Security Manager administrators, add devices, edit policies, view reports—access the full functionality of the NetScreen-Security Manager system.

Configuring UI Preferences

You can configure preferences for UI behavior, such as appearance, external tool use, polling statistics, and UI timeout. For details on configuring these settings, see the topics under “NetScreen-Security Manager User Interface” in the NetScreen-Security Manager Online Help.

UI Overview

The NetScreen-Security Manager User Interface (UI) appears after you log in, and displays a set of menus and toolbar icons at the top of the UI window. Depending on the component displayed, right-click menus are available to perform various tasks. The UI is shown below:
Navigation Tree
The navigation tree displays the 11 NetScreen-Security Manager modules in the left pane of the NetScreen-Security Manager window. Double-click a module to display its contents in a hierarchical tree format. For details on each module, see below.

Main Display Area
The main display area displays content for the selected module or module contents.

- Menu Bar—The menu bar contains clickable commands. You can access many menu bar commands using keyboard shortcuts such as add, edit, delete. For a complete list of keyboards shortcuts, see the NetScreen-Security Manager Online Help.
- ToolBar—The toolbar contains buttons for common tasks. The buttons displayed in the toolbar are determined by the selected module.
- Status Bar—The status bar displays additional information for selected module.

NetScreen-Security Manager Modules
The navigation tree contains 11 top-level modules that contain specific NetScreen-Security Manager functionality, as detailed in the following sections.
Log Viewer

The Log Viewer displays log entries that your security devices generate based on criteria that you defined in your Security Policies, on the GUI Server, and in the device configuration. Log entries appear in table format; each row contains a single log entry, and each column defines specific information for a log entry.

You can customize the view (which log entries and what log information is shown) using log filters or by changing the column settings.

Use the Log Viewer to:

- View summarized information about security events and alarms
- Drill down to view information about a specific log entry
- Show, hide, or move columns to customize the Log Viewer
- Filter log entries by column headings
- Create and save custom views that display your filters/column settings
- Set flags on Log Viewer entries to indicate a specific priority or action

For more details on using the Log Viewer, see Chapter 12, “Logging”.

Report Manager

The Report Manager contains summary, graphs, and charts that detail specific security events that occur on your network. NetScreen-Security Manager generates reports to visually represent the information contained in your log entries. You can use reports to quickly summarize security threats to your network, analyze traffic behavior, and determine the efficiency of NetScreen-Security Manager. To share reports or to use report information in other application, you can print or export report data.

Log Investigator

The Log Investigator contains tools for analyzing your log entries in depth. Use the Log Investigator to:

- Manipulate and change constraints on log information
- Correlate log entries visually and rapidly
- Filter log entries while maintaining the broader picture

Device Manager

The Device Manager contains the device objects that represent your security devices. You can create:

- Security devices and systems—The devices you use to enable access to your network and to protect your network against malicious traffic.
- Vsyst devices—A vsys is a virtual device that exists within a physical security device.

- Clusters—A cluster is two security devices joined together in a high availability configuration to ensure continued network uptime.

- Vsyst cluster—A Vsyst cluster device is vsys device that has a cluster as its root device.

- Extranet devices—Firewalls or VPN devices that are not Juniper Networks security devices.

- Templates—A template is a partial device configuration that you can define a single time then use for multiple devices.

- Device Groups—A device group is a user-defined collection of devices.

Security Policies
Security Policies contains the firewall, multicast, and VPN rules that control traffic on your network. Using a graphical, easy-to-use rule building platform, you can quickly create and deploy new policies to your security devices.

Use Security Policies to:
- Add or modify existing Security Policies
- Add or modify existing VPN rules
- Create new policies based on existing policies
- Install policies on one or multiple security devices
- Delete policies

If the device configurations that you imported from your security devices contained policies, Security Policies displays those imported policies. For details on editing those imported polices or creating new policies, see Chapter 9, “Configuring Security Policies” or Chapter 10 “Configuring VPNs”.

VPN Manager
The VPN Manager contains the VPN abstractions that control the VPN tunnels between your managed devices and remote users. Using VPN objects such Protected Resources and IKE Proposals, you can create multiple VPNs for use in your Security Policies.

Use the VPN Manager to:
- Define the protected resources on your network. Protected Resources represent the network resources you want to protect in a VPN.
- Create custom IKE Phase 1 and 2 Proposals.
Configure AutoKey IKE, L2TP, and L2TP-over-AutoKey IKE VPNs in policy-based or route-based modes. You can also create an AutoKey IKE mixed mode VPN to connect policy-based VPN members with route-based VPN members.

Configure AutoKey IKE and L2TP policy-based VPNs for remote access services (RAS) and include multiple users.

Object Manager

The Object Manager contains the Objects used in your NetScreen-Security Manager system. An object is a re-usable, basic NetScreen-Security Manager building block that contains specific information; you use objects to create device configurations, policies, and VPNs. All objects are shared, meaning they can be shared by all devices and policies in the domain.

You can create the following objects in NetScreen-Security Manager:

- Address Objects—Represent components of your network (hosts, networks, servers)
- Schedule Objects—Represent specific dates and times. You can use schedule objects in firewall rules to specify a time or time period that the rule is in effect.
- DI Profiles—Define the attack signature patterns, protocol anomalies, and the action you want a security device to take against matching traffic.
- IDP Attack Objects—Attack patterns that detect known and unknown attacks. You use IDP attack objects within IDP rules.
- AV Objects—Represent the servers that contain your virus definitions and AntiVirus software.
- Web Filtering Objects (URL Profiles)—Define the URLs, the URL categories, and the action you want a security device to take against matching traffic.
- Service Objects—Represent services running on your network, such as FTP, HTTP, and Telnet. NetScreen-Security Manager contains a database of Service Objects for well-known services; you can also create new Service Objects to represent the custom services you are running on your network.
- User Objects—Represent the remote users that access the network protected by the security device. To provide remote users with access, create a user object for each user, then create a VPN that includes those user objects.
- IP Pools—Represent a range of IP addresses. You use IP pools when you configure a DHCP Server for your managed devices.
- Authentication Servers—Represent external authentication servers, such as RADIUS and SecurID servers. You can use an authentication server object to authenticate NetScreen-Security Manager admins (RADIUS only), XAuth users, IKE RAS users, and L2TP users.
- Group Expressions—Are OR, AND, and NOT statements that set conditions for authentication requirements.
Remote Settings—Represent DNS and WINS servers. You use remote settings object when configuring XAuth or L2TP authentication in a VPN.

NAT Objects—Represent MIPs, VIPs, and DIPs.

GTP Objects—Represent GTP client connections.

CA Objects—Represent the certificate authority’s certificate.

CRL Objects—Represent the certificate authority’s certificate revocation list.

You can use the Object Manager to:

- View and/or edit the Object properties
- Create, edit, or delete Objects
- Create custom groups of Objects

For more details on objects, see Chapter 8, “Configuring Objects”.

Server Manager

Server Manager contains server objects that represent your management system components. Use Server Manager to manage and monitor the individual server processes that comprise your NetScreen-Security Manager system.

Realtime Monitor

Realtime Monitor provides a graphical view of the current status of all devices managed by NetScreen-Security Manager:

- Device Monitor—Tracks the connection state and configuration state of your security devices. You can also view device details to see CPU utilization and memory usage for each device, or check device statistics.

- VPN Monitor—Tracks the status of all VPN tunnels.

- NSRP Monitor—Tracks the status of NSRP.

You can customize Realtime Monitor to display only the information you want to see, as well as update information at specified time periods. You can also set alarm criteria for a device or process. For more details on Realtime Monitor, see Chapter 11, “Monitoring”.

Job Manager

Job Manager contains the status of commands (also called directives) that NetScreen-Security Manager sends to your managed devices. You can view summaries or details for active jobs and completed jobs. For more details on Job Manager, refer to “Tracking Device Updates” on page 406.
Audit Log Viewer
The Audit Log Viewer contains a log entry for every change made by a NetScreen-Security Manager administrator. For more details on Audit Log Viewer, see “Using the Audit Log Viewer” on page 764.

Action Manager
The Action Manager enables you to forward logs on a per domain basis. For more details on using the Action Manager, refer to “Using the Action Manager to Forward Logs by Domain” on page 770.

Validation Icons in the User Interface
NetScreen-Security Manager uses automatic validation to help you identify the integrity of a configuration or specific parameter with just a simple glance. The following icons may appear as you work in the UI:

Table 4: Validation Status for Devices

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error</td>
<td>Indicates that a configuration or parameter is not configured correctly in the NetScreen-Security Manager UI. Updating a device with this modeled configuration causes problems on the device.</td>
</tr>
<tr>
<td>Warning</td>
<td>Indicates that a configuration or parameter is not configured correctly in the NetScreen-Security Manager UI. Updating a device with this modeled configuration might cause problems on the device.</td>
</tr>
<tr>
<td>Needs Validation</td>
<td>Indicates that a configuration or parameter has not been validated. Although NetScreen-Security Manager automatically validates all parameters when entered, this icon might appear for a template-driven value after you have changed a template. Juniper Networks highly recommends that you validate all parameters before updating a device.</td>
</tr>
<tr>
<td>Valid</td>
<td>Indicates that a configuration or parameter is configured correctly in the NetScreen-Security Manager UI.</td>
</tr>
</tbody>
</table>

Validation and Data Origination Icons
Data origin tooltips show the user where field data originates. These are implemented as additional types of validation messages (beyond the current Error and Warning messages), adding Template Value, Override, and From Object messages. Each has its own icon and text color in the tooltips.

Table 5: Validation Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Message Type</th>
<th>Meaning</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error</td>
<td>Indicates that a configuration or parameter is not configured correctly in the NetScreen-Security Manager UI. Updating a device with this modeled configuration causes problems on the device.</td>
<td>Highest</td>
<td></td>
</tr>
<tr>
<td>Warning</td>
<td>Indicates that a configuration or parameter is not configured correctly in the NetScreen-Security Manager UI. Updating a device with this modeled configuration might cause problems on the device.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
From Object messages only appear when viewing template objects to help find fields set in the template.

When more than one type of icon appears within a panel, the highest priority icon appears next to the icon in the tree and the panel title bar.

Working with Other NetScreen-Security Manager Administrators

When multiple NetScreen-Security Manager admins are accessing the NetScreen-Security Manager system at the same time, NetScreen-Security Manager ensures that all edits are synchronized by locking an active object. Only one admin at a time can edit existing values for an object, but multiple admins can still view the existing values for that object.

- When an NetScreen-Security Manager admin begins editing an object, the UI locks that object to prevent other admins from editing the object’s value.

- During lockout, NetScreen-Security Manager makes “lazy” saves of all edits made and stores them in an in-memory database. If NetScreen-Security Manager crashes during a lazy save, edits made since the last lazy save are lost, and NetScreen-Security Manager prompts the NetScreen-Security Manager admin to rollback to the last lazy save.

- When the admin completes and saves the edit, that object is unlocked, enabling other admins to edit it. However, because the UI does not immediately refresh the object values, you must manually refresh the UI to view the most recent versions.

When you attempt to open a locked object, a warning message appears indicating that the object is locked and can be opened only as a read-only object. The warning message also contains the name of the NetScreen-Security Manager administrator that is currently editing the object. Depending on your administrator privileges, you can locate contact information for the admin in the Manage Administrators and Domains area of the UI (From the file menu, select Tools > Manage Administrators and Domains). For details on working with administrators and domains, see “Configuring Role-Based Administration” on page 57.
For example, let’s say Bob and Carol are both NetScreen-Security Manager admins with the same roles. If both admins view the same object, but Bob also edits and saves the object, NetScreen-Security Manager **does not** notify Carol that a newer version of the object exists. To see the newest version, Carol must first close, then open the object again or refresh the console.

### Searching in the User Interface

You can use the integrated search feature in NetScreen-Security Manager to quickly locate a specific setting within a UI screen or dialog box.

To locate a word, simply begin typing the word and the search window automatically appears in the top left of the selected screen or dialog box. The UI attempts to match your entry to an existing value; as you enter more characters, the UI continues to search for a match. Use the arrow keys to move between each matching value. If your entry appears in red, no matching value was found within the selected screen or dialog box.

To locate a different data type, such as an IP address, change the search mode. To display all available search modes, press the backslash key (\). The search mode window appears, as shown below.

**Figure 4: UI Search Modes**

<table>
<thead>
<tr>
<th>Select Mode:</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[C]</td>
<td>- find pattern inside entire search string.</td>
</tr>
<tr>
<td>[S]</td>
<td>- search for value starts with pattern.</td>
</tr>
<tr>
<td>[R]</td>
<td>- use a Regular Expression to find a value.</td>
</tr>
<tr>
<td>[I]</td>
<td>- search for an IP. &quot;**&quot; notation is allowed.</td>
</tr>
</tbody>
</table>

Press the key that represents the search mode you want to use, then begin entering the search criteria. Switching to another view or pressing the ESC key ends the search operation and closes the tool window. The following sections detail each search mode.

**Contains String [C] Search Mode**

Use to locate a pattern anywhere in a string. For example, to locate the pattern “RPC” in Service Objects:

1. In the main navigation tree, select Object Manager > Service Objects > Predefined Service Objects, then select the Service Object icon at the top of the Service Tree tab.

2. Press the backslash key (\) to display the search mode window.

3. Enter C, then enter RPC. The UI automatically highlights the first match, MS-RPC-ANY, as shown below.
Chapter 1: Introduction to NetScreen-Security Manager

Working in the User Interface

Figure 5: “Contains String” Search Mode Example

Table 1: Predefined Service Objects

<table>
<thead>
<tr>
<th>Service Tree</th>
<th>Service Table</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Search for:</strong> rpc</td>
<td></td>
</tr>
<tr>
<td>MS-IMSERV (predefined)</td>
<td></td>
</tr>
<tr>
<td>MS-MESSENGER (predefined)</td>
<td></td>
</tr>
<tr>
<td>MS-MQVM (predefined)</td>
<td></td>
</tr>
<tr>
<td>MS-NETLCGON (predefined)</td>
<td></td>
</tr>
<tr>
<td>MS-RPC-ANY (predefined)</td>
<td></td>
</tr>
<tr>
<td>MS-RPC-EPN (predefined)</td>
<td></td>
</tr>
</tbody>
</table>

Starts With [S] Search Mode

Use to locate a pattern at the beginning of a string. For example, to locate the pattern “OR” in security devices:

1. In the main navigation tree, select Device Manager > Security Devices, then select the security devices icon at the top of the Device Tree window.

2. Press the backslash key (\) to display the search mode window.

3. Enter S, then enter OR. The UI automatically highlights the first match, OR_EU_208, as shown below:

Figure 6: “Starts With” Search Mode Example

Table 2: FW/VPN Devices

<table>
<thead>
<tr>
<th>FW/VPN Device Tree</th>
<th>FW/VPN Device List</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Starts With:</strong> or</td>
<td></td>
</tr>
<tr>
<td>CA_SV_208_A</td>
<td></td>
</tr>
<tr>
<td>CA_SV_JSG2000</td>
<td></td>
</tr>
<tr>
<td>ID_BO_25</td>
<td></td>
</tr>
<tr>
<td>MT_BT_500</td>
<td></td>
</tr>
<tr>
<td>OR_EU_208</td>
<td></td>
</tr>
<tr>
<td>OR_PT_5XT</td>
<td></td>
</tr>
<tr>
<td>WA_0Y_2...</td>
<td></td>
</tr>
</tbody>
</table>

Regular Expression [R] Search Mode

Use to locate a value using a regular expression. For example, to locate all attack objects that detect denial-of-service attacks:

1. In the main navigation tree, select Object Manager > Attack Objects, then select the Predefined Attacks tab.

2. Select the first entry in the column Name, then press the backslash key (\) to display the search mode window.
3. Enter R, then enter the following characters: DoS|enial. The following figure details this expression:

Figure 7: “Regular Expression” Search Mode Details

![Diagram showing the use of regular expressions: The pipe character (|) represents an OR relationship. The period character (.) represents any character. In this example, you are searching for word “denial” or “Denial”.

The UI automatically highlights the first match; click the down arrow key to highlight the next match. Both matches are shown below:

Figure 8: “Regular Expression” Search Mode Example

<table>
<thead>
<tr>
<th>Predefined Attacks</th>
<th>Predefined Attack Group</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Match 1</strong></td>
<td><strong>Match 2</strong></td>
</tr>
<tr>
<td><img src="image1.png" alt="Example" /></td>
<td><img src="image2.png" alt="Example" /></td>
</tr>
</tbody>
</table>

**NOTE:** The regular expression search mode supports all common regular expressions. For more information about regular expressions, consult a dedicated resource. Mastering Regular Expressions, 2nd Edition, by Jeffrey E. F. Friedl is a good start.

**IP [I] Search Mode**

Use to locate an IP address. For example, to locate the IP address 6.6.6.60 and 6.6.6.61 in Address Objects:
1. In the main navigation tree, select Object Manager > Address Objects, then select the Address Table tab.

2. Select the first entry in the column IP/Domain Name, then press the backslash key (\) to display the search mode window.

3. Enter I, then enter 6.6.6.*. The UI automatically highlights the first match, 6.6.6.60. Click the down arrow key to highlight the next match, 6.6.6.61.

When searching in a table, your search criteria is applied only to the selected column. If you select a different column, such as Name, and perform the same search, your results differ. Both search results are shown below:

Figure 9: “IP Address” Search Mode Example

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>IP/Domain Name</th>
<th>Netmask</th>
</tr>
</thead>
<tbody>
<tr>
<td>global3</td>
<td>Host</td>
<td>5.5.5.50</td>
<td>32</td>
</tr>
<tr>
<td>untrust1</td>
<td>Host</td>
<td>5.5.5.50</td>
<td>32</td>
</tr>
<tr>
<td>global1</td>
<td>Host</td>
<td>6.6.6.60</td>
<td>32</td>
</tr>
<tr>
<td>global2</td>
<td>Host</td>
<td>6.6.6.61</td>
<td>32</td>
</tr>
<tr>
<td>trust_net</td>
<td>Network</td>
<td>10.1.1.0</td>
<td>24</td>
</tr>
<tr>
<td>test1</td>
<td>Host</td>
<td>10.1.1.5</td>
<td>32</td>
</tr>
<tr>
<td>kayak</td>
<td>Host</td>
<td>10.1.1.76</td>
<td>32</td>
</tr>
<tr>
<td>Internal Network</td>
<td>Network</td>
<td>10.10.1.1</td>
<td>24</td>
</tr>
<tr>
<td>Web Server</td>
<td>Host</td>
<td>10.10.1.255</td>
<td>32</td>
</tr>
<tr>
<td>FTP Server</td>
<td>Host</td>
<td>10.10.10.254</td>
<td>32</td>
</tr>
<tr>
<td>trust_ian</td>
<td>Network</td>
<td>10.100.2.0</td>
<td>24</td>
</tr>
</tbody>
</table>

New Features for NetScreen-Security Manager 2005.3

This release of Netscreen-Security Manager contains the following new features and enhancements.

Supported Security Devices and Versions of ScreenOS

This release of NetScreen-Security Manager supports the following new security devices and ScreenOS versions:
ScreenOS 5.3—You can now manage Juniper Networks security devices running ScreenOS 5.3. This includes the following new features:

- QoS/Virtual Interface Enhancements—You can now configure DSCP value and Provisioned Bandwidth.
- 10-VLAN on NS-5GT Trust-Untrust Mode Support—You can now configure multiple VLANs on the NS-5GT running ScreenOS 5.3.
- Dual-DMZ Port Mode on the NS-5GT—You can now configure Dual-DMZ port modes on the NS-5GT and NS-5GTWLAN running ScreenOS 5.3. Refer to for more information.
- Source-Based Routing (SBR)/Source Interface-Based Routing (SIBR) with Next-Hop as Virtual Router Enhancements—You can now configure virtual routers as the next-hop on security devices running ScreenOS 5.3. Refer to for more information.
- Support for ScreenOS 5.0 DIAL features—There is a new Route failover option. When the Route option is selected, NetScreen-Security Manager activates the Virtual Router IP Address and Network Mask fields to specify the route to be used for failover monitoring. In addition, a validation condition needs to be added to check that the entered IP/Mask corresponds to an actual route on the specified virtual router.

NetScreen-Security Manager System and UI

This release of NetScreen-Security Manager includes the following new features, changes, and enhancements in the NetScreen-Security Manager system and UI.

- Forward Support of Future ScreenOS Releases
- Trial License Keys
- Rule-Based Log Actions
- Domain-Based Log Actions
- Simplified Logs
- Viewing and Monitoring Devices from the Global Domain
- Juniper Networks InfraNet Controller Support
- Enhanced Certificate Support
- Enhanced Antivirus Support
- Antispam Capabilities
- Enhanced Template Administration
- Enhanced Deep Inspection
- BGP Soft Reconfiguration
- Multiple MIP Support
- ALG Enhancements for VoIP
- Policy Filter Tool
- Enhanced Certificate Support
- URL Filtering Renamed “Web Filtering”
- Adding Static DNS Host Addresses

Forward Support of Future ScreenOS Releases
NetScreen-Security Manager now provides management support for security devices running future versions of ScreenOS. After installing a schema patch for a future version of ScreenOS, you can upgrade support for the device using the UI. For some new ScreenOS commands, you can then issue Supplemental CLI to configure new features on security devices running future versions of ScreenOS. Supplemental CLI is supported for ScreenOS 5.1 and higher.

Trial License Keys
You can now install a License Key on a security device running ScreenOS 5.3 (or later) enabling you to use subscription-based features on a trial basis.

Rule-Based Log Actions
You can now configure log actions (i.e., Run Script, Send Email, Syslog Messages, SNMP Trap, Write CSV, Write XML) on a per rule basis within a security policy.

Domain-Based Log Actions
A new tree node called “Action Manager” appears in the UI enabling you to configure log actions and criteria for device logs on a per domain basis.

Simplified Logs
Using the Log Viewer, you can now view specific log entries describing device connect and disconnect events.

Viewing and Monitoring Devices from the Global Domain
A new column called “Domain” appears in the Realtime Monitor (Device Monitor and NSRP Monitor) enabling you to monitor security devices across all domains from the global domain. Two new columns called “From Domain” and “To Domain” appear in the VPN Monitor enabling you to monitor security devices across all domains from the global domain.
Juniper Networks Infranet Controller Support
A new setting called “Infranet Settings” now appears in the Device Manager enabling you to configure security devices to work with Juniper Networks Infranet Controllers. You can use Infranet Controllers to segregate your network based on user privileges as well as the security level of the user’s system.

Enhanced Certificate Support
Generated certificates now support Domain Component (DC= ) entries.

Enhanced Antivirus Support
Antivirus settings can be created and applied at the template level. Scanning is configurable based on application protocol, file extension/mime type, and compression level. Email notifications of found viruses is also supported.

Antispam Capabilities
Netscreen-Security Manager now supports whitelist/blacklist antispam capabilities. Emails can be blocked or tagged based on email ID, hostname, domain name, or IP address.

Enhanced Template Administration
The Template Operations dialog provides sophisticated template administration capabilities. Each operation can affect multiple templates and devices. It has the following capabilities:

- assign one or more templates
- remove one or more templates
- validate templates against devices, either after updating device data or as a standalone action
- remove existing device values that conflict with values in the template
- report template values that are irrelevant to the device(s)
- report values that conflict between the directive-specified template and the template previously assigned to the device.

Enhanced Deep Inspection
Deep Inspection now covers all the protocols covered by IDP. In addition, multiple types of signature packages are now supported, such as server protection, client protection, and worm mitigation.

BGP Soft Reconfiguration
A dynamic inbound soft reset is used to generate inbound updates of a routing table from a peer. An outbound soft reset is used to send a new set of updates to a peer.
Multiple MIP Support
You can now add multiple MIPs to the Device Server. When a device is added, the NetScreen-Security Manager administrator has the choice of selecting the desired MIP for each device.

ALG Enhancements for VoIP
This release includes enhanced SIP Settings for ALG configuration as well as new H.323 settings and MGCP settings.

Policy Filter Tool
This tool provides the ability to filter policy rules based on one or more filter conditions specified for rule attributes. One filter can contain several filter conditions for different attributes. The filter only applies to the currently selected rulebase and does not affect other open clients. The filter results are displayed in the same rulebase. Rules that do not match filter conditions are hidden. In the firewall rulebase only open rule groups are filtered. When a filter is set and a closed rule group is expanded, only rules that match the filter will be displayed in the group.

Enhanced Certificate Support
Allows certificate with DC in certificate DN to be used for dialup user IKE ID selection.

URL Filtering Renamed “Web Filtering”
The term “URL Filtering” is now referred to as “Web Filtering.”

Adding Static DNS Host Addresses
This ScreenOS 5.3 feature lets you create a static host name with multiple IP addresses. You can use this feature to create dynamic addressing in NSM. In some cases, a common firewall policy is desired but due to differences in the IP addressing at different sites, it is impossible to share the policy. Using the static host entries and address objects, this can be accomplished. Each device would contain a local mapping of hostname to IP, but the policy would contain address object referencing the hostname. This allows the firewall policy to focus on the application as opposed to the specific IP addressing.
Chapter 2
Getting Started

Security devices are the Juniper Networks security components that you use to enable access to your network components and to protect your network against malicious traffic. When you use NetScreen-Security Manager to manage your security devices, you are creating a virtual network that represents your physical network. Using this virtual network, you can create, control, and maintain the security of your physical network at a system-level.

This chapter provides information to help you decide how best to create your virtual network and simplify management tasks.

The following sections are in this chapter:

- Overview: Configuring Security Devices
- Overview: Configuring IDP-Capable Devices
- Simplifying Management
Overview: Configuring Security Devices

A firewall provides perimeter and boundary protection using data encryption, authentication, access control, and some attack detection and prevention. Firewalls and virtual private networks (VPNs) are designed for high speed operation at the network layer. In NetScreen-Security Manager, Juniper Networks firewall and VPN devices are known as security devices, and are the security components that you use to enable access to your network components and to protect your network against malicious traffic.

To manage Juniper Network security devices that already exist on your network, you can import their device configurations into NetScreen-Security Manager. Each imported device appears in the NetScreen-Security Manager UI, where you can view or make changes to the device, such as change settings in the device configuration, edit the security policy for the device, and upgrade device firmware.

For new devices that do not yet exist on your network, you can create their device configuration in NetScreen-Security Manager. When you physically deploy your device, you can install the modeled device configuration on that device to instantly get it up and running. After you install the modeled configuration on the device, you can manage the device just as you would an imported device.

A third option, Migration, exists for devices that are currently managed by NetScreen-Global PRO or Global PRO Express. For complete information on NetScreen-Security Manager migration, see the NetScreen-Security Manager 2004 FP2 Migration Guide.

Importing Existing Devices

For networks with deployed security devices, if you have already designed, staged, and set up a working physical device already, you don’t need to do that again; you can simply import that device so it exists (virtually) inside the management station. This import includes the routing, IP configuration, access and Security Policies, access privileges, and other device-specific information defined on the device.

To import and configure your existing devices:

1. Add the security device and import your device configuration.

   a. In the NetScreen-Security Manager main navigation tree, select Device Manager > Security Devices.

   b. In the main display area, click the Add icon and select Add Device. Follow the instructions in the Add Device Wizard to import the security device.

   As NetScreen-Security Manager imports the existing device configuration, it automatically creates all objects and policies in the configuration.
2. Verify the imported device configuration and related information:
   - Run a Delta Config Summary and view the results.
   - Check Device configuration information.
   - Check Address, Service, Schedule, and NAT Objects
   - Check Security Policies
   - Check Protected Resources
   - Check VPNs

3. Correct any validation errors, if found, and check for duplicate objects (such as address objects, custom service objects). Be sure to consolidate any duplicate objects before importing another security device.

You can also delete devices from NetScreen-Security Manager, and re-import them if necessary. Deleting a device removes all device configuration information from the management system, but might be the best solution if you need to perform extensive troubleshooting and/or reconfigure the device locally. After you have made the necessary changes locally, you can then re-import that device into the NetScreen-Security Manager system.

For details on importing devices, see Chapter 4, “Adding Devices”.

**Modeling New Devices**

For new networks or networks that do not use a previously deployed Juniper Networks security device, you should review your network topology thoroughly and design a security system that works for your organization.

When creating a new security network using NetScreen-Security Manager:

1. Create the domain structure that best suits your network topology and access requirements.

2. Create NetScreen-Security Manager administrators and set their permission level by creating and assigning roles.

3. Add your security devices and create their device configurations. You’ll need to define zones, assign interfaces, and designate virtual routers to enable the firewall to pass traffic on the network.

   - Use templates to configure multiple devices. Templates help you re-use common information to quickly create configurations for similar devices.

**NOTE:** NetScreen-Security Manager does not import IDP rulebases in a Security Policy when importing the device configuration.
For ScreenOS 5.x devices, you can use Rapid Deployment (RD) to deploy multiple devices in non-technical locations. Use RD to stage and configure devices quickly, then simultaneously update all device with policies to control traffic as desired in multiple locations.

4. Create the objects used in your Security Policies. These objects might include:
   - NAT Objects for policy-based network address translation
   - Address Objects for your network components
   - Service Objects for your custom network services (NetScreen-Security Manager includes an object database of common transport and application-level services).
   - AV objects for detecting viruses in your network traffic
   - GTP objects for inspecting GTP packets.

5. Create Security Policies. NetScreen-Security Manager integrates policy management, linking multiple security device to one Security Policy that defines the type of traffic permitted on the network and how that traffic is treated inside the network.
   - Add a policy, then create firewall rules that specify source, destination, service, and action. You can also create multicast rules to handle multicast control traffic. Select the devices that should receive and implement this rule in the Install On column.
   - Verify each policy using the Policy Validation tool.

6. Update devices
   - Resolve any validation issues with the device configuration
   - View a summary of the device configuration to ensure that all device parameters are correct.
   - Check progress in Job Manager

7. Create VPN Rules
   - Create Protected Resources
   - Create User Objects and User Groups for RAS VPNs
   - Use VPN Manager to select VPN members, then automatically generate the rules for each member

For details on adding devices, see Chapter 4, “Adding Devices”; for details on configuring devices, see Chapter 5, “Configuring Devices”.
Overview: Configuring IDP-Capable Devices

While firewalls provide basic protection, they are not designed to detect all attacks. Advanced attack methods often elude firewall detection by embedding the attack within permitted traffic or using attack vectors that are outside the firewall’s detection capability.

Juniper Networks Intrusion Detection and Prevention (IDP) technology can both detect and then stop attacks when deployed inline to your network. Unlike IDS, IDP uses multiple methods to detect attacks against your network and prevent attackers from gaining access and doing damage. IDP can drop malicious packets or connections before the attacks can enter your network. IDP is designed to reduce false positives and ensure that only actual malicious traffic is detected and stopped. You can also deploy IDP as a passive sniffer, similar to a traditional IDS, but with greater accuracy and manageability.

Supported IDP-Capable Devices

NetScreen-Security Manager supports IDP as part of a ISG 2000 and ISG 1000 security systems running ScreenOS 5.0.0-IDP1. The ISG 2000 and ISG 1000 security module is an optional component installed in the device that provides IDP functionality. If you purchased an ISG 2000 or ISG 1000 device that does not have IDP capability, you can upgrade the device to be an IDP-capable system by replacing the memory chip in the CPU, installing up to three security modules, and installing the Advanced and IDP license keys for IDP. See the ISG 2000 Field Upgrade document or the ISG 1000 IDP Field Upgrade Guide for instructions on how to upgrade to include IDP capabilities.

You can use the ISG 2000 or ISG 1000 device with IDP capability as a fully-integrated FW/VPN/IDP security system that not only screens traffic between the Internet and your private network, but also provides application-level security. Or, use the ISG 2000 or ISG 1000 device as a dedicated IDP system to protect critical segments of your private network, such as Web servers or corporate accounting servers.

NOTE: Juniper Networks offers IDP Sensors, which are standalone appliances that provide IDP functionality without integrated FW/VPN capabilities. However, you cannot use the NetScreen-Security Manager system to manage IDP Sensors; NetScreen-Security Manager 2005.3 supports IDP only on the ISG 2000 and ISG 1000 devices.

NetScreen-Security Manager is the sole means for configuring and managing IDP on the ISG 2000 and ISG 1000 devices. Although you can use ScreenOS CLI or WebUI to configure the firewall and VPN capabilities of the security device, you must use the NetScreen-Security Manager UI to enable and configure IDP capabilities on the security module.

Enabling IDP Functionality

To enable the IDP functionality on the security device and deploy that functionality to protect your network, you must perform the following:

1. Add the ISG 2000 or ISG 1000 security device
2. Install IDP and Advanced License Keys
3. Update Attack Objects
4. Create Address Objects (optional)
5. Configure a Security Policy for IDP
6. Review IDP Logs

The following sections detail each step.

**Adding the ISG 2000 or ISG 1000 Security Device with Security Module**

You must add an ISG 2000 or ISG 1000 security device with at least one security module to the NetScreen-Security Manager UI before you can enable the IDP functionality in security module.

NetScreen-Security Manager automatically detects the security module when you:

- Import an ISG 2000 or ISG 1000 device running ScreenOS 5.0.0-IDP1 and the security module is already installed.
- Install a security module in an existing ISG 2000 or ISG 1000 device that is currently managed by NetScreen-Security Manager, then upgrade the device firmware to ScreenOS 5.0.0-IDP1.

**NOTE:** *After you have upgraded the firmware, you must re-import the device configuration.*

To view the security module in the UI, open the device configuration and select Network > Chassis.

If you purchased an ISG 2000 or ISG 1000 device with only FW/VPN capabilities, you can upgrade the device to an IDP-capable system by replacing the memory chip in the CPU, installing up to three security modules, and installing the Advanced and IDP license keys.

**Installing License Keys**

To access the IDP functionality on a security module, you must install both an Advanced license key and an IDP license key on the security device. For details on obtaining and installing a license key, see “Managing License Keys” on page 414.

**NOTE:** *Installing the IDP license key disables the Deep Inspection (DI) feature.*
Updating Attack Objects

You must update the attack object database and the attack detector engine on the ISG 2000 or ISG 1000 security device before you can use the IDP functionality on the security module. To update the database and detector engine, you download new attack objects from the attack object database server to the GUI Server, then download the new objects to your managed devices. The detector engine is automatically included in the attack object update file.

To update the attack object database on the NetScreen-Security Manager GUI Server:

1. From the Tools menu bar, select Preferences. The New Preferences dialog box appears. In the preference navigation tree, select Attack Object.
2. In the Download URL box, ensure that the URL of the Attack Object Database server is as follows:

   https://services.netscreen.com/restricted/sigupdates/nsmfp3-DI-IDP/NSMFP3-DI-IDPAttackUpdateInfo.dat

3. Click OK to apply your settings.
4. From the menu bar, select Tools > Update NSM Attack Database. The Update NSM Attack Database dialog box appears.
5. Follow the instructions in the Attack Update Manager to download the new Signature and Protocol Anomaly Attack Objects to the NetScreen-Security Manager GUI Server. The management system contacts the server and downloads the latest database version to the GUI Server.

After you have updated the attack object database on the GUI Server, you can use that database to update the attack object database on your managed devices.

To download the attack object database update to your managed devices:

1. From the menu bar, select Devices > Deep Inspection > Update Device Attack Database. The Update Device Attack Database dialog box appears.
2. Click Next, then select the managed devices on which you want to install the attack object update.
3. Follow the directions in the Change Device Sigpack wizard to update the attack object database on the selected managed devices.

NOTE: You must have enabled DNS on the NetScreen-Security Manager GUI server before you can update your attack objects.

NOTE: To perform a local update, see “Preparing for a Local Update” on page 416.
Adding Objects
Create Address Objects for the network components you want to protect with IDP. These components can be routers, servers, workstations, subnetworks, or any other object connected to your network. You can also create address object groups, which represent multiple address objects. (If you have previously created network objects for use with your FW/VPN security devices, you do not need to create them again.)

For details on creating address objects, see “Configuring Address Objects” on page 444.

Configuring a Security Policy for IDP
Because the security module on the device processes traffic after the FW/VPN management module, you must configure a firewall rule to pass permitted traffic to the IDP rulebases. Enabling IDP functionality in a Security Policy is a two-step process: first enable a firewall rule to pass permitted traffic to the IDP rulebases, then create the IDP rules that detect and prevent malicious traffic from entering your network.

When creating a new Security Policy for your IDP deployment, we highly recommend you use a Security Policy template. Each Security Policy template contains the IDP rulebase and IDP rules that use the default actions associated with the Attack Object severity and protocol groups. You can customize these rules to work on your network as needed, such as selecting your own Address Objects as the Destination IP and choosing IDP actions and notifications that reflect your security needs.

If you do not use a Security Policy template, you must add the IDP rulebase manually, as detailed in “Adding the IDP Rulebases” on page 41.

Configure Firewall Rules
You can enable IDP within an existing rule, or create a new rule. Configure the firewall rule as you would normally, setting the source/destination zones, address objects, services, and so on to define the type of network traffic you want to permit.

When configuring the firewall rule, consider the following:

- Traffic that is denied by a firewall rule cannot be passed to IDP rules. To enable IDP in a firewall rule, the action must be permit.
- When deploying the ISG 2000 or ISG 1000 device as a dedicated IDP system, configure a single firewall rule that directs all traffic to the IDP rules. (By default, the firewall denies all traffic).

---

NOTE: When operating the security device in a non-transparent mode, you must have configured basic security device settings, such as assigning interfaces to zones, setting the administrative password, and configuring default routes. For details on configuring these settings, see the User Guide that shipped with the device.

When operating the security device in transparent mode for and using as a dedicated IDP system, you do not need to configure additional firewall settings.
For firewall rules that pass traffic to the IDP rulebases, the Install On column must include IDP-capable devices only.

**Setting the IDP Mode**

Because the security module is part of the inline security device, IDP protects your network while directly in the path of traffic coming and going on your network.

To set the IDP mode:

1. In the main navigation tree, select Security Policies, then double-click the policy name in the Security Policies window. The firewall rulebase appears.
2. In the Rule Options column of a firewall rule, select IDP.
3. Select one of the following modes:

   - In **inline** mode, IDP is directly in the path of traffic on your network and can detect and block attacks. For example, you can deploy the ISG 2000 or ISG 1000 with integrated FW/VPN/IDP capabilities between the Internet and an enterprise LAN, WAN, or special zones such as DMZ.

   - In **inline tap** mode, IDP can detect attacks and provide notification. IDP receives a copy of a packet while the original packet is forwarded on the network. IDP examines the copy of the packet and flags any potential problems. IDP’s inspection of packets does not affect the forwarding of the packet on the network.

**NOTE:** You must deploy the ISG 2000 or ISG 1000 device inline. You cannot connect a device that is in inline tap mode to an external TAP or SPAN port on a switch.

Selecting either mode enables IDP for the firewall rule, and configures the security device to forward all permitted traffic to the IDP rulebases for further processing.

**Adding the IDP Rulebases**

After you have enabled one or more firewall rules to pass traffic to the IDP rulebases, you must add one or more of the following IDP rulebases to the Security Policy:

- **The IDP Rulebase**—This is the main rulebase for IDP rules. Add this rulebase when you want to configure rules that use attack objects to detect specific malicious or anomalous activity in your network traffic.

   For a quick overview of creating rules in the IDP rulebase, see the following section (page 40); for complete details, see “Configuring IDP Rules” on page 556.

- **The Exempt Rulebase**—This rulebase works in conjunction with the IDP rulebase. When traffic matches a rule in the IDP rulebase, the security module attempts to match the traffic against the Exempt rulebase before performing the specified action or creating a log record for the event.

Add the Exempt rulebase:
When an IDP rule uses attack object groups containing one or more attack objects that produce false positives or irrelevant log records.

To exclude a specific source, destination, or source/destination pair from matching an IDP rule (prevents unnecessary alarms).

When the IDP rulebase uses static or dynamic attack object groups that contain one or more attack objects that produce false positives or irrelevant log records.

For details on creating rules in the Exempt Rulebase, see “Configuring Exempt Rules” on page 568.

The Backdoor Detection Rulebase—This rulebase detects backdoor traffic from components on your internal network. A “backdoor” is a mechanism installed on a host computer that facilitates unauthorized access to the system. Attackers who have already compromised a system often install a backdoor to make future attacks easier. However, when attackers type commands to control a backdoor, they generate interactive traffic that your security device can detect.

Add this rulebase to your Security Policy when you want to configure rules that detect backdoor activity on your internal network. For details on configuring rules in the Backdoor Detection Rulebase, see “Configuring Backdoor Rules” on page 572.

NOTE: NetScreen-Security Manager does not import IDP rulebases in a Security Policy when importing the device configuration from an existing IDP-capable security device.

If you are using Security Policy template, the IDP rulebases are automatically added to the policy. However, if you are not using a template, you must manually add the IDP rulebases to your policy.

To add the IDP, Exempt, or Backdoor Detection rulebase:

1. In the main navigation tree, select Security Policies, then double-click the policy name in the Security Policies window.

2. Click the Add icon in the upper right corner of the Security Policy window and select Add < IDP, Exempt, or Backdoor Detection > Rulebase. The selected rulebase tab appears.

Configure IDP rules

IDP detection and prevention capabilities work against attacks by dropping connections during the attack detection process, preventing attacks from reaching the target system.

To add a rule to a rulebase:

1. Click the rulebase tab for the rulebase in which you want to add a rule.

2. On the left side of the Security Policy window, click the Add icon. A default rule appears.
For rules in the IDP rulebase, you define the type of network traffic to monitor, the attacks to detect, the action to be taken against matching traffic, and the notification you want to receive. Specifically, you must configure the following:

- **Configure Match Criteria**—Define the type of network traffic you want the IDP security module to monitor for attacks, such as source/destination zones, source/destination address objects, and the application layer protocols (services) supported by the destination address object. You can also negate zones, address objects, or services.

You configure the match criteria in the following IDP rulebase columns:

- From Zone
- Source
- To Zone
- Destination
- Service

For details on configuring match criteria within the IDP rulebase, see “Defining Match For IDP Rules” on page 557.

- **Add Attack Objects**—Add the attacks you want the IDP security module to match in the monitored network traffic. Each attack is defined as an attack object, which represents a known pattern of attack. Whenever this known pattern of attack is encountered in the monitored network traffic, the attack object is matched. You can add attack objects by groups (category, operating system, severity, and so on) or individually.

You configure attack objects within the Attack column of the IDP rule:

- For details on selecting attacks within IDP rules, see “Configuring Attack Objects in IDP Rules” on page 563
- For details on IDP attack objects, see “Working with IDP Attack Objects” on page 453.
- For details on creating your own custom IDP attack objects, see “Configuring Custom DI/IDP Attacks” on page 456.

- **Configure Action**—Define the action the IDP security module takes when a particular attack is detected. You can define an IDP action (action that the security module takes against the current connection) and an IP action (action that the security module takes against the current and future connections to or from the same IP address).

You configure IDP actions in Action column of an IDP rule. For details, see “Defining Actions For IDP Rules” on page 562.
You configure IP actions in the IP Action column of an IDP rule. For details, see “Configuring IP Actions in IDP Rules” on page 565. (The IP Action column appears only when viewing the Security Policy in Expanded Mode. To change the view mode of a policy, from the menu bar, select View > Expanded Mode or Compact Mode).

- Configure Notification—Define the logging and notification activities you want the IDP security module to take when the IDP rule is matched. You can configure the module to generate log entries, trigger alarms, and log captured packets.

You configure Notification settings in the Notification column of an IDP rule. For details, see “Configuring Notification in IDP Rules” on page 566.

Assign, Validate, and Install the Security Policy

After you have created the necessary firewall and IDP rules within the Security Policy, you must perform the following to apply the policy to your network traffic:

1. Assign the policy to a device—Assigning a policy to a device links the device to that policy, enabling NetScreen-Security Manager to install the policy on that device. To assign an existing policy to the ISG 2000 or ISG 1000 device:
   a. In Device Manager, right-click the ISG 2000 or ISG 1000 device and select Policy > Assign Policy.
   b. Select the security policy you just created.

2. Validate the Security Policy (Optional)—Validating a Security Policy can identify potential problems before you install it. To validate a policy:
   a. From the menu bar click Devices > Policy > Validate Policy.
   b. A Job Manager window appears to display job information and progress. If NetScreen-Security Manager identifies any problems in the policy during policy validation, it displays information about the problem at the bottom of the selected rulebase. For example, if you included a non-IDP capable security device in the Install On column of an IDP rule, policy validation displays an error message.

3. Install the Security Policy—During policy installation, NetScreen-Security Manager installs the entire Security Policy, including the firewall and IDP rules, on the security devices you selected in the Install On column of each rule. To install a policy:
   a. From the menu bar click Devices > Configuration > Update Device Config.
   b. In the Update Devices dialog box, select the ISG 2000 or ISG 1000 security device, then click OK.
   c. A Job Manager window appears to display job information and progress.
Review IDP Logs

After you have enabled IDP on the device and installed a Security Policy that uses IDP detection and prevention functionality, IDP logs begin to appear in the NetScreen-Security Manager Log Viewer (assuming you enabled IDP logging for each IDP rule). Depending on the attack objects you included in the IDP logging, the IDP log entries you receive might detail events such as attacks against your network, protocol anomalies, or even simple login attempts.

To view IDP log entries, in the main navigation tree, select Log Viewer > DI/IDP Logs. The Log Viewer displays all IDP logs generated by the security device.

NOTE: The DI/IDP Logs view is a predefined custom view applied to all log entries received by NetScreen-Security Manager. To view all log entries for all devices in the selected domain without filters, select the Log Viewer module in the main navigation tree.

We recommend you review and analyze these log entries to determine the effectiveness of your current Security Policy and IDP rules. Log entries are often a valuable insight into your network traffic. You can see where traffic is coming from, where traffic is going to, and what malicious content (if any) the traffic contains.

Maintaining IDP

Attackers are constantly devising new and better ways to infiltrate your network. Juniper Networks is busy too, discovering these new attacks and creating new attack objects to detect them—so you can prevent the attacks from entering your network. To ensure that the IDP security module and that your Security Policy remains highly effective against all emerging and evolving threats, we highly recommend that you perform frequent updates to the attack object database and to the IDP detection engine, as detailed below.

Updating the Attack Database

The attack object database stored on an IDP-capable security device contains predefined attack objects and groups designed to detect known attack patterns and protocol anomalies within network traffic. You use these attack objects when configuring IDP rules in a Security Policy for a security device.

Juniper Networks updates the predefined attack objects and groups on a regular basis with newly-discovered attack patterns. You can update the attack object database on your security devices by downloading the new attacks and groups to the NetScreen-Security Manager GUI Server, then installing the new database on your security devices.

Updates to the attack object database can include:

- New descriptions or severities for existing attack objects
- New attack objects
- Deletion of obsolete Attack Objects
For details on updating the attack object database, see “Managing the Attack Database” on page 415.

**Updating the IDP Detector Engine**

The IDP engine is dynamically changeable firmware that runs on the ISG 2000 or ISG 1000 security device running ScreenOS 5.0.0-IDP1. Automatic updates to the IDP engine occur when you:

- Upgrade Security Device Firmware—When you upgrade the firmware on a ISG 2000 or ISG 1000 device running 5.0 IDP, the upgraded firmware includes the most recent version of the IDP engine as well as a new version of ScreenOS.

- Update Attack Database From GUI Server—When you update attack objects on the security device using the GUI Server, you also automatically update the IDP engine on the device. Because attack database updates are available more often than firmware releases, an attack database update may include a more recent version of the IDP engine than is available on the latest firmware release. For example, an attack database update may contain updated IDP attack objects that can only be used with an updated version of the IDP engine.

Updating the IDP Detector Engine does not require you to reboot the device.

You can also manually update the IDP Detector Engine. However, the IDP engine version you install on a ISG 2000 or ISG 1000 device must be compatible with the version of the firmware that is running in the device.

**NOTE:** You cannot downgrade the IDP engine version on the device.

For details on updating the IDP Detector Engine, see “Updating the IDP Detector Engine” on page 420.

**Creating IDP-Only Administrators**

You can use NetScreen-Security Manager’s role-based administration (RBA) to create a custom role for administrators working with IDP functionality on a security device. For example, if your organization’s IDS or IDP administrators do not configure FW/VPN security devices, you can restrict administrative privileges for those admins within the NetScreen-Security Manager system to IDP tasks only.

**NOTE:** The NetScreen-Security Manager “super” admin automatically has all IDP-related permissions.

A custom role for IDP administrators might include the following permissions:

- Attack Update
- Create/View/Edit/Delete Policies
- Create/View/Edit/Delete Backdoor and IDP Rulebases
- View Firewall Rulebases
Simplifying Management

When you add your security devices to NetScreen-Security Manager, you are creating the network organization that you use to manage your security system. Before you begin the device creation or device import process however, first review your network topology and decide how you want it to appear in NetScreen-Security Manager. This is particularly important when you are creating a new network, but is also helpful when you are importing networks, as you might want to edit your network design to take advantage of key NetScreen-Security Manager management features.

These features include:

- Using Device Groups
- Using Device Templates
- Merging Policies
- Using a Naming Convention

Using Device Groups

You can create groups of devices to manage multiple devices at one time. Group your device by region, device type, or even OS version, then use the groups to:

- Deploy new or updated device configurations to the entire device group
- Deploy new or updated policies to the entire device group
- Create reports using the log information from the entire device group

Using Device Templates

A template is a predefined device configuration that helps you re-use common information. A domain can contain multiple templates, and you can use templates to quickly configure and deploy multiple devices. A device template looks much like a device configuration—the template page displays boxes for interfaces, zones, and virtual routers in which you can enter values. When you add a new device that uses similar information as a previously added device, you can use a device template to fill in specific configuration values so you do not have to re-enter information.

For example, you might create a generic NetScreen-5XT template that you can use each time you add a device of that type. Or, you can apply multiple templates to the same device. You can map a maximum of 63 templates to the same device; you set the priority of the template to determine the order in which they applied.
For example, you might create the following templates:

- DNS setting template
- Default PKI Settings template
- Authentication template

Then, apply these template to a single device to instantly configure the DNS, PKI, and Authentication settings for the device.

NOTE: You cannot create VPNs between devices in different domains.

Merging Policies

You can create new policies for all your managed devices from the central NetScreen-Security Manager UI and deploy them with a single click. Alternatively, NetScreen-Security Manager can import all existing policies from your security device. You can import all security and access policies from your security devices, and import all VPN tunnels (route-based and policy-based) from your security devices.

Each time you import a policy from a managed device, that policy appears in NetScreen-Security Manager as a separate, individual policy in the Security Policies list. To simplify policy management and maintenance, you can merge two policies into a single policy. For details on merging policies, see Chapter 9, "Configuring Security Policies".

Using a Naming Convention

A naming convention is a method for assigning names to your network devices (firewalls, servers, workstations, and so on) that enables you to quickly identify where the device is and what its purpose is.

If your network is small, you might choose a simple naming convention, such as planets, Science Fiction, cars, mountains. When using this type of informal method to name your network components, be sure to choose a theme that is easily understood by both your users and administrators, and that still has room to grow. For example, you might use the naming convention. <city>_<name>, with a naming theme of Greek mythology figures; some sample device names might be la_ns5gt_Athena, sf_ns5XT_Zeus, oak_ns204.

If your network is larger, however, you need a more formal naming schema that is more descriptive of the network component's location and purpose. Having a logical and standardized naming convention can help you quickly identify the appropriate administrator for the component, as well as quickly identify the component location of without having to tear through the subnet tables.

A typical naming convention for large, distributed networks consists of a standardized location identification code, followed by the department code, a description of function, and a numerical sequence.
EXAMPLE: USING A NAMING CONVENTION FOR SECURITY DEVICES
You use the naming convention: nation_state_city_platform_name for your security
devices. Your devices use names similar to the following:

- us_ca_la_ns5gt_01
- us_co_dv_ns204_05
- us_tx_hs_ns5200_10

EXAMPLE: USING A NAMING CONVENTION FOR ADDRESS OBJECTS
For address objects that represent networks or hosts, you use the following naming
convention: city_function_service_00:

- City—A two-character postal abbreviation for the city where the server resides.
- Function—Some common functional abbreviations:
  - SV (Server)
  - WS (Workstation)
  - IIS (Web Server)
  - MSX (Mail Server)
  - SQL (SQL Server)
  - SMS (SMS Server)
  - APP (Application Server)
- Service—Abbreviated name of the main service on that machine.
- Number—A sequential number starting with 01.

For example, the first Apache Web server installed in Los Angeles would read:
la_ws_apache_01.

For address objects that represent client hosts, use the naming convention:
city_flastname_(m or w)_os

- City—A two-character postal abbreviation for the office location the user is
  attached to.
- FLastname—The first initial and last name of the main user (or general account
  name if it is a multiuser machine)
- (M or W)—A single letter to designate Mobile computer or Workstation
- OS—A two-character abbreviation for the operating system.

For example, Wendy Parker, working in Houston on a Windows 2000 Pro laptop,
would see her machine name as: hs_wparker_m_2kpro.
Simplifying Management
Chapter 3
Configuring Role-Based Administration

This chapter details how to use Juniper Networks NetScreen-Security Manager’s role-based administration feature to configure domains, administrators, and roles to manage your network. Your organization probably already has an existing permission structure that is defined by job titles, responsibilities, and geographical access to your security devices. Using role-based administration, you can re-create this same permission structure in NetScreen-Security Manager.

RBA is particularly useful for Enterprise and Service Provider organizations that have different administrative roles associated with managing a large network and security infrastructure. You can create custom roles with specific permissions to create the exact administration structure your organization requires.

After you have created a role-based administrative structure for your network, you can begin thinking about your central management strategy and how to prepare your network for NetScreen-Security Manager. NetScreen-Security Manager includes many features specifically designed for managing multiple Juniper Networks security devices, such as device groups, templates, and so on.

The following sections are in this chapter:

- About Role-Based Administration (RBA)
- Using Role-Based Administration Effectively
- Configuring Role-Based Administration
About Role-Based Administration (RBA)

NetScreen-Security Manager’s role-based administration feature enables you to define strategic roles for your administrators, delegate management tasks, and enhance existing permission structures with new task-based functionality.

Use NetScreen-Security Manager to create a security environment that reflects your current offline administrator roles and responsibilities. Because management is centralized, it’s easy to configure multiple administrators for multiple domains. By specifying the exact tasks your NetScreen-Security Manager administrators can perform within a domain, you minimize the probability of errors and security violations, and enable a clear audit trail for every management event.

About Domains

A domain is a logical grouping of devices, their Security Policies, and their access privileges. A domain can contain devices, templates, objects, policies, VPNs, administrators, activities, authentication servers, groups—a representation of all or a subset of the physical devices and functionality on your network.

NetScreen-Security Manager contains a default top-level domain, called the global domain, which can contain additional domains, called subdomains. Use subdomains to manage multiple domains in a single hierarchical structure. You can create all your devices and their configurations in the global domain, or you can configure additional subdomains within the global domain.

NOTE: You can create only one level of subdomains in NetScreen-Security Manager.

Typically, multiple domains are used for two main reasons: to define network structure and to control administrator access. Multiple domains help to separate large, geographically distant systems into smaller, more manageable sections, and also to control administrative access to individual systems.

For example, a small organization might only have one domain (the global domain) for their entire network, while a large, international organization might have dozens of subdomains that exist within the global domain to represent each of its regional office networks across the world. A Service Provider might use domains to build a virtual network for each client network, then assign access permissions for each client domain to the appropriate client administrator.

Domain selection is critical if you plan to use VPNs in your network. Because you can create VPNs only between devices in the same domain, be sure to add the devices you want to connect with a VPN to the same domain, or use the workaround detailed on “Domain selection is critical when using VPNs. You can create VPNs only between devices within the same domain. If you need to add a device to a VPN in a different domain, add the device as an extranet device in the domain that contains the VPN, then add the extranet device to the VPN (as shown in Figure 13).”.
About Roles

Roles define who can perform which task and view which information. NetScreen-Security Manager uses a powerful, role-based access control system that enables you to create custom roles for individual administrators. Use role-based management to control administrative access to NetScreen-Security Manager functionality.

All NetScreen-Security Manager users are some type of admin. During NetScreen-Security Manager installation, you are prompted for a password for the (default) admin account for NetScreen-Security Manager; this admin account is the first administrator, and is therefore the super administrator. The super admin automatically has all permissions, and can create other domains, admins, and roles. As super admin, you specify who has what permissions for NetScreen-Security Manager functionality for the entire NetScreen-Security Manager system, a single domain, or specific functionality within a domain.

NOTE: All passwords handled by NetScreen-Security Manager are case-sensitive.

You can define multiple NetScreen-Security Manager administrators and assign dedicated roles to each administrator:

- A role is a set of activities that specify the functions the admin can perform.
- Activities are predefined tasks within NetScreen-Security Manager; the NetScreen-Security Manager admin can combine multiple activities into a custom role.

NOTE: You cannot define a custom activity.

With role-based administration, you can specify who has what permissions for NetScreen-Security Manager functionality for the entire NetScreen-Security Manager system, a single domain, or even specific functionality within a domain. You can even delegate NetScreen-Security Manager administrator management, enabling existing NetScreen-Security Manager administrators to create other NetScreen-Security Manager administrators, assign domains, and define or create roles.

NOTE: A device administrator is the person responsible for managing a device directly, using ScreenOS (command line or WebUI). If a device administrator uses only ScreenOS to manage devices, do not create an NetScreen-Security Manager administrator account for the device admin; however, if a device administrator uses both ScreenOS and NetScreen-Security Manager to manage devices, you must create a NetScreen-Security Manager administrator account for the device admin.

Using Role-Based Administration Effectively

The structure of your NetScreen-Security Manager domains should reflect both your existing network structure and your desired permission structure.
Network Structure—Use multiple domains to segregate large, geographically distant networks into locally-managed sections.

Permission Structure—Use multiple domains to segregate critical devices and systems from less important network areas, then restrict administrator access to devices in the critical domain.

Your organization probably already has an existing permission structure that is defined by job titles, responsibilities, and geographical access to your security devices. You can re-create this same permission structure in NetScreen-Security Manager.

Role-based administration is particularly useful for Enterprise and Service Provider organizations that have different administrative roles associated with managing a large network and security infrastructure. RBA is also helpful for any size organization that wants to provide access to other device statistics to non-administrators within the organization, such as creating a role for the CIO to access reports.

Enterprise Organizations

Each enterprise defines administrative roles differently. With NetScreen-Security Manager, you have the flexibility to create the appropriate permission level.

Geographical Divisions

To manage large, geographically diverse networks, you can create domains for each separate geographical location. Typically, the larger the Enterprise, the deeper and more complex your geographical divisions. Two common geographical divisions are Corporate and Region:

- Corporate—The corporate domain is the global domain. In the global domain, the super administrator creates the devices, objects, and policies that exist in the corporate network, and creates subdomains for each region.

- Region—Each region is a subdomain. Within each subdomain, the super admin creates a regional administrator to manage the subdomain. The super admin also specifies the roles the regional admin has to view and manipulate devices, remote users, configuration actions, and report information within that subdomain.

NOC and SOC

To ensure continual network uptime and provide prompt respond to network attacks, each geographical division is often monitored by a dedicated Network Operations Center (NOC) and/or Security Operations Center (SOC). The NOC and SOC are typically the same location for small organizations, but might be physically separate for larger, more complex organizations. Whether combined or separate, NOC and SOC administrators perform distinct roles:

- NOC administrators focus on network connectivity and status.

- SOC administrators focus on network attacks and events associated with Security Policies.
Administrator Types

Many organizations have different types of administrators for different roles within the company. Each organization has a unique vision for the granularity of their permission structure.

Tiered NOC/SOC

Typically, a NOC/SOC uses a 3-tier permission structure. The administrators in each tier have a specific level of skill and understanding of the underlying network and technology, as well as access permissions to view or change configurations. An example NOC/SOC center might use the following role structure:

- Tier 1 administrators view events and audit configurations.
- Tier 2 administrators view events and audit configurations, but also change network configurations during troubleshooting.
- Tier 3 administrators have full access to all functionality on the device, and make configuration and policy changes.

Configuration Responsibilities

Some enterprise organizations use different administrator groups to manage specific aspects of device configuration. Configuration responsibilities might use the following role structure:

- IT group—Integrates new devices into the existing network infrastructure. This group has roles with activities for setting up Layer 2 and Layer 3 aspects of the device (IP addressing, Routing, Vlans, Syslog, and so on). Within the IT group, the network administrator might also have a role with an activity for managing the management system.
- Security group—Creates and manages Security Policies. This group has roles with activities for defining custom services, address objects, and firewall rules on devices for which they have responsibility.
- Remote Connectivity group—Creates and manages VPNs and RAS user configuration. This group has roles with activities for configuring VPNs and remote users.

Specific Tasks

- Configuration Validation—An audit administrator approves all configuration changes before those changes are made on the network. Only the auditor has a role with activities for updating devices on the network.
- Reporting—A reporting administrator views reports for one or more domains. A regional reporting administrator has a role with activities for viewing reports for their regional subdomain; a corporate reporting administrator has a role with activities for viewing reports for the global domain and all subdomains.
- Configuration Update—An update administrator updates firmware for all security devices. The update administrator has a role with activities for updating firmware on the devices in their assigned domain.
Administrative Management—A management administrator creates new administrators and manages their permissions. The super administrator creates an management administrator to delegate administrator management. For example, a NOC Tier 2 administrator has a role that includes the activity to create new admins, but cannot assign them an activity that is not included in their own role. Typically, a subdomain has only one management administrator to control the creation of administrators.

Device Installation—A device install admin creates new devices. The device install administrator has a role with activities for adding, updating, and viewing device configurations.

Service Providers

Service Providers can use NetScreen-Security Manager domain, subdomains, and roles to manage their internal infrastructure and their customers’ infrastructures.

Internal Network

Internally, a Service Provider network is similar to an enterprise network; both view their networks as regions with dedicated NOC/SOC, and both use the same types of administrators.

Managed Security Service Provider (MSSP)

Telcos and Service Providers use their networks to generate revenue. Customers pay the MSSP to deploy devices and to manage the VPN or FW infrastructure. MSSPs use different role structures that best match their organizational structure:

- MSSP owns devices; customer manages infrastructure
- Customer owns devices; MSSP manages infrastructure
- Customer leases devices; MSSP manages the infrastructure
- MSSP owns devices and manages infrastructure (Customer Network Management (CNM))

CNM Service Providers vary widely in how they control access to their customer networks. Some CNMs assign one or more customers to a network administrator that has control over the device and policies used by those customers. Other CNMs assign one network administrator to view reports for all customers. CNMs might use the following role structure:

- Super administrator. At the global domain, the super administrator creates
  - The internal network of the CNM.
  - A subdomain for each customer. The customer subdomain contains the devices and objects that belong to the customer network. Because the customer network is completely contained within a subdomain, it is isolated from other subdomains for other customers.
Customer administrators to manage one or more subdomains. The super administrator assigns roles to the customer administrator in one or more customer subdomains, enabling the customer admin to handle multiple customer networks without access to the CNM internal network.

Additionally, the super administrator can create a role structure that maps to the specific tasks performed by each customer administrator, as described in “Specific Tasks”.

MSSPs can also use Virtual Systems (available on NetScreen-500 and -5000 series) to share a single device between multiple customers. For each customer, the MSSP creates a customer subdomain and a virtual system within that subdomain.

Configuring Role-Based Administration

When you have analyzed your network and permission structure and designed your domain strategy, you are ready to create subdomains and new NetScreen-Security Manager administrators for those subdomains. When you create NetScreen-Security Manager administrators for your subdomains, you can set their permissions so that they can see only the domains to which they have access.

From the menu bar, click Tools > Manage Administrators and Domains to display the role-based administration settings for NetScreen-Security Manager:

- Administrators—Configure administrators for NetScreen-Security Manager.
- Roles—View or edit default roles, or create your own custom roles for your NetScreen-Security Manager admins.
- Subdomains—Create subdomains to segregate networks.
- Current Domain Detail—View the information about the current domain, such as assigned administrators, authentication method, and default authentication servers.

The following sections detail how to configure these role-based administration settings.

NOTE: When migrating from Juniper Networks NetScreen-Global PRO or Global PRO Express, you can migrate your existing domain structure and administrators. For details, see the NetScreen-Security Manager 2004 FP2 Migration Guide.

Creating Administrators

The super administrator automatically has full permissions for all subdomains, so you don’t need to assign new subdomains to the super administrator. However, to assign the subdomain to another administrator, you must first create the administrator and specify their permissions within a selected subdomain.

You can create NetScreen-Security Manager administrators at the global domain level or at the subdomain level:
To assign the new admin permissions in the global domain or permissions in multiple subdomains, create the admin in the global domain.

To assign the new admin permissions in only one subdomain, create the admin in that subdomain.

Configuring General Settings
To create a NetScreen-Security Manager administrator, click the Add icon in the Administrator tab to display the New Admin dialog box. In the General tab, enter a name and contact information (email, phone, and other basic information) for the new administrator.

NOTE: The following characters are not supported for NetScreen-Security Manager administrator names:

- Dot character ( . )
- Number sign ( # )
- Dollar sign ( $ )
- Asterisk ( * )
- Ampersand ( & )
- Circumflex ( ^ )

Configuring Authorization
To configure the authorization method for the new administrator, click the Authorization tab and select local or remote authentication:

- For locally authenticated administrators, the NetScreen-Security Manager management server handles authentication. You must specify the password that NetScreen-Security Manager uses to authenticate the admin; the admin must enter this password at the NetScreen-Security Manager UI login screen.

NOTE: All passwords handled by NetScreen-Security Manager are case-sensitive.

- For remotely authenticated administrators, a RADIUS authentication server handles authentication. Because the admin password is stored on the RADIUS server, you do not need to enter the password again, however, the admin must enter the password at the NetScreen-Security Manager UI login screen.
To configure the RADIUS authentication server for NetScreen-Security Manager administrators, see the NetScreen-Security Manager Online Help topic “Editing the Domain Contact.”

---

**NOTE:** The super administrator has immutable powers. You cannot change or delete permissions for the super administrator; you can, however, change the password for the super admin. Because this admin has complete control over NetScreen-Security Manager functionality, we recommend that you consider the security of the super administrator password appropriately. If you forget or lose the super administrator password, please contact Juniper Networks technical support.

---

**Configuring Permissions**

To assign permissions to the new admin, click the Permissions tab and select a role for the new admin. A role is a collection of predefined activities that define access to NetScreen-Security Manager functionality. When you assign a role to a NetScreen-Security Manager admin, the admin can perform the predefined system activities specified in that role.

You can select a default or custom role for that administrator. NetScreen-Security Manager includes default roles for common job responsibilities:

- **Domain Administrator**—Can perform all activities in the domain
- **Read-Only Domain Administrator**—Can perform all read-only activities in the domain
- **System Administrator**—Can perform all system-wide activities and Domain Administrator activities
- **Read-Only System Administrator**—Can perform all read-only system-wide activities and Domain Administrator activities

Each default role contains activities that relate to the traditional responsibilities for a specific job title. Use a default role to quickly create NetScreen-Security Manager administrators, or when your organization’s existing permission structure maps closely to the permissions defined in the default role.

All roles, default and custom, are created from activities. In a default role, the activities are chosen for you; in a custom role, you choose the activities that make up the desired functionality. For details on creating custom roles, see “Creating Roles”.

---

**NOTE:** Role assignment is additive. When you assign multiple roles to a single admin, the permissions specified by the activities in the role are added.

---

You must also select a domain. You can assign admins to the global domain, or to one or more subdomains (the subdomain must already exist). Administrators must log in to the domain they were created in. For example, the super admin has access to all domains, but must log in to the global domain first, then switch to a subdomain using the domain menu. For details on creating a subdomain, see “Creating Subdomains”.
Creating Roles

Click the Roles tab to display available roles. NetScreen-Security Manager includes four default roles, as described above, and can contain an unlimited number of custom roles.

Creating Custom Roles

For more complex and diverse permissions requirements, create custom roles to specify the exact level of permission you want to give an admin. An activity is a predefined task that defines access to a function in NetScreen-Security Manager. To assign one or more activities to an NetScreen-Security Manager admin, create a role that includes those activities and assign the role to the admin.

Some activities are dependant on other activities. If you select a dependant activity, NetScreen-Security Manager automatically selects the prerequisite activities. You can clear prerequisite activities from a custom role, but doing so affects permissions granted in the dependant activity. For example, if you create a role that includes the activity “Create VPNs”, the activities “Edit VPNs” and “View VPNs” are automatically selected for you.

Click the Add icon to display the New Role dialog box and all available activities. NetScreen-Security Manager includes 75 predefined activities, grouped by similar functionality.

Table 6: Predefined NetScreen-Security Manager Administrator Activities

<table>
<thead>
<tr>
<th>Function</th>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action Attributes</td>
<td>View Modify</td>
<td>The Action Manager is a node on the main navigation tree that enables you to configure the management system to forward logs generated within a specific domain or subdomain.</td>
</tr>
<tr>
<td>Admin Roles</td>
<td>View Create Edit Delete</td>
<td>An admin role defines the access privileges for a NetScreen-Security Manager administrator.</td>
</tr>
<tr>
<td>Admins</td>
<td>View Create Edit Delete</td>
<td>An admin is a user of the NetScreen-Security Manager management system.</td>
</tr>
<tr>
<td>Attack Update</td>
<td>N/A</td>
<td>This activity enables an admin to update the attack object database on the NetScreen-Security Manager system and on each managed device that supports Deep Inspection.</td>
</tr>
<tr>
<td>Audit Logs</td>
<td>View</td>
<td>An audit log records an administrative change (such as login, update, or policy change) to the managed devices or management system.</td>
</tr>
</tbody>
</table>
### Configuring Role-Based Administration

<table>
<thead>
<tr>
<th>Function</th>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backdoor Rulebase</td>
<td>Create</td>
<td>This activity enables an admin to manage the Backdoor Rulebase within a Security Policy. Rules configured in this rulebase are supported only on IDP capable security devices, such as the ISG 2000 or ISG 1000 running 5.0IDP1.</td>
</tr>
<tr>
<td></td>
<td>Edit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>View</td>
<td></td>
</tr>
<tr>
<td>CLI-based Reports</td>
<td>N/A</td>
<td>This activity enables an admin to generate predefined and shared historical log reports using the guiSvrCli command utility.</td>
</tr>
<tr>
<td>CLI-based Security Update</td>
<td>N/A</td>
<td>This activity enables an admin to update the attack object database on the NetScreen-Security Manager system using guiSvrCli command utility.</td>
</tr>
<tr>
<td>Device Certificates</td>
<td>Generate and Upload</td>
<td>A device certificate authenticates packets passing through a device.</td>
</tr>
<tr>
<td></td>
<td>Get</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Delete</td>
<td></td>
</tr>
<tr>
<td>Device Configuration</td>
<td>View</td>
<td>A device configuration is the modeled configuration that exists for a managed device within NetScreen-Security Manager.</td>
</tr>
<tr>
<td></td>
<td>Update</td>
<td></td>
</tr>
<tr>
<td>Device Delta Config</td>
<td>View</td>
<td>A device delta config is a report that details the differences between the device configuration running on the physical device and the modeled device configuration in NetScreen-Security Manager.</td>
</tr>
<tr>
<td>Device Firmware</td>
<td>Update</td>
<td>The device firmware is the ScreenOS software image used on the managed device.</td>
</tr>
<tr>
<td>Device Log Comments</td>
<td>Update</td>
<td>A device log comment is a user-defined description of a security event that is recorded in a device log.</td>
</tr>
<tr>
<td>Device Log Flags</td>
<td>Update</td>
<td>A device log flag is visual icon that can be assigned to a device log. Admins can assign flags to indicate severity, status, and other options to a device log.</td>
</tr>
<tr>
<td>Device Logs</td>
<td>View</td>
<td>A device log records a security event that occurred on a security device.</td>
</tr>
<tr>
<td></td>
<td>Hide and Unhide</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Purge</td>
<td></td>
</tr>
<tr>
<td>Device Passwords</td>
<td>View</td>
<td>This activity enables an admin to view device passwords in configuration summaries and Job Manager information details. Note: All passwords handled by NetScreen-Security Manager are case-sensitive.</td>
</tr>
<tr>
<td>Device Reboot</td>
<td>Reboot</td>
<td>A device reboot is a reboot command sent to a managed device to power down, then power up.</td>
</tr>
<tr>
<td>Function</td>
<td>Task</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>---------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Device Running Config</td>
<td>View</td>
<td>A device running config is a report that details the device configuration running on the physical device.</td>
</tr>
<tr>
<td>Device Software Keys</td>
<td>Install</td>
<td>A device software key provides enhances or adds functionality for a managed device.</td>
</tr>
<tr>
<td>Device Status Monitor</td>
<td>View</td>
<td>The device status monitor tracks the status security devices, VPN tunnels, and NSRP.</td>
</tr>
<tr>
<td>Device URL Category</td>
<td>Update</td>
<td>The device URL category list contains predefined URL categories used in Web filtering profiles. You can update the device URL category list from the system URL category list.</td>
</tr>
<tr>
<td>Devices, Device Groups, and Templates</td>
<td>View</td>
<td>A device is a security device.</td>
</tr>
<tr>
<td></td>
<td>Create</td>
<td>A device group is a collection of managed devices.</td>
</tr>
<tr>
<td></td>
<td>Edit</td>
<td>A template is a device configuration that contains predefined, static configuration information, such as networking settings, interface settings, or DNS settings.</td>
</tr>
<tr>
<td></td>
<td>Delete</td>
<td></td>
</tr>
<tr>
<td>Firewall Rulebases</td>
<td>Create/Edit View</td>
<td>The firewall rulebases (Zone and Global) in a Security Policy contain rules that handle traffic passing through the firewall. These activities enable an admin to control and/or view rules in the firewall rulebases.</td>
</tr>
<tr>
<td>HA for guiSvrClusterMgr</td>
<td>N/A</td>
<td>An historical log report is a report generated using historical log entries. If an admin can view historical log reports, then that admin can also view shared historical log reports and their definitions.</td>
</tr>
<tr>
<td>Historical Log Reports</td>
<td>View</td>
<td></td>
</tr>
<tr>
<td>IDP Rulebase</td>
<td>Create</td>
<td>This activity enables an admin to manage the IDP Rulebase within a Security Policy. Rules configured in this rulebase are supported only on IDP capable security devices, such as the ISG 2000 or ISG 1000 running 5.0IDP1.</td>
</tr>
<tr>
<td></td>
<td>Edit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>View</td>
<td></td>
</tr>
<tr>
<td>Investigative Log Reports</td>
<td>View</td>
<td>The Log Investigator generates investigative log reports based on selected criteria. This activity enables an admin to view those log reports.</td>
</tr>
<tr>
<td>Job Status Logs</td>
<td>Purge</td>
<td>Each time NetScreen-Security Manager performs a task for which a job is created, Job Manager creates a job status log. This activity enables an admin to purge those logs from the management system.</td>
</tr>
</tbody>
</table>

62  Configuring Role-Based Administration
### Chapter 3: Configuring Role-Based Administration

<table>
<thead>
<tr>
<th>Function</th>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jobs</td>
<td>View</td>
<td>A job is a task that NetScreen-Security Manager performs, such as updating a device, generating a device certificate request, and importing a device.</td>
</tr>
<tr>
<td>Multicast Rulebases</td>
<td>Create/Edit View</td>
<td>The multicast rulebase in a Security Policy contains multicast rules, which can handle IGMP and PIM-SM traffic. These activities enable an admin to control and/or view rules in the multicast rulebase.</td>
</tr>
<tr>
<td>NSRP Monitor</td>
<td>View</td>
<td>NSRP Monitor tracks NSRP statistics. To enable NetScreen-Security Manager to track these statistics, you must enable &quot;NSRP Monitor&quot; in the NSRP properties for each cluster device.</td>
</tr>
<tr>
<td>Security Policies</td>
<td>View</td>
<td>A policy is a set of rules that determines how a device handles traffic passing through the firewall.</td>
</tr>
<tr>
<td></td>
<td>Create</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Edit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Delete</td>
<td></td>
</tr>
<tr>
<td>Policy Lookup Table</td>
<td>Modify</td>
<td>A rulebase in a Security Policy contains rules that manage specific types of traffic passing through the managed device. These activities enable an admin to delete a rulebase.</td>
</tr>
<tr>
<td>Rulebases</td>
<td>Delete</td>
<td>A rulebase in a Security Policy contains rules that manage specific types of traffic passing through the managed device. These activities enable an admin to delete a rulebase.</td>
</tr>
<tr>
<td>Servers</td>
<td>View</td>
<td>The Device Server and GUI Server comprise the NetScreen-Security Manager System.</td>
</tr>
<tr>
<td></td>
<td>Create</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Edit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Delete</td>
<td></td>
</tr>
<tr>
<td>Shared Historical Log Report</td>
<td>View</td>
<td>A shared historical log report is a user-defined historical log report that is available to users with the appropriate permissions in a domain. These reports appear under “Shared Reports” in the UI and can be generated offline with the guiSvrCli utility. If an admin can create shared historical log reports, then that admin can also move a report from “My Reports” to “Shared Reports. An admin requires permission to delete shared historical log reports in order to move a report from “Shared Reports” to “My Reports”.</td>
</tr>
<tr>
<td></td>
<td>Create</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Edit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Delete</td>
<td></td>
</tr>
<tr>
<td>Shared Objects and Groups</td>
<td>View</td>
<td>An object contains re-usable information. Shared objects include address book objects, schedule objects, attack objects, service objects, and user objects.</td>
</tr>
<tr>
<td></td>
<td>Create</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Edit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Delete</td>
<td></td>
</tr>
<tr>
<td>Subdomains and Groups</td>
<td>View</td>
<td>A subdomain is a separate, unique representation of other networks that exist within your larger network.</td>
</tr>
<tr>
<td></td>
<td>Create</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Edit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Delete</td>
<td></td>
</tr>
</tbody>
</table>
Assigning and Viewing Custom Roles

When you create an administrator, you can assign a custom role just as you would a default role. However, you cannot assign an activity or role that you do not possess to another admin (the activity or role is not visible in the list of available activities or roles).

Within a domain, you can view only the custom roles that you have created or that have been assigned to you. You cannot view custom roles created by other administrators, even if the role is in the same domain and includes the same activities already assigned to you.

Creating Subdomains

To create a subdomain, in the Subdomains tab, add a new subdomain and click apply. The new subdomain appears in the subdomain list.

NOTE: You cannot create VPNs between devices in different domains,
You can add unlimited subdomains in the global domain, however, you cannot create subdomains within a subdomain. Additionally, when you view the Manage Domains and Administrators dialog box from within a subdomain, the Subdomains tab does not appear. To view a subdomain in the main display area, select it from the pull-down menu at the top of the navigation tree.

NOTE: Objects and groups defined in the global domain are not visible in subdomains.

Viewing Current Domain Detail

The domain detail displays the subdomains, administrators, their roles, and authentication server for the currently selected domain (subdomains appear only when in the global domain).

You can designate a default RADIUS authentication server for the global domain and for each subdomain. The default auth server is used:

- To authenticate administrators when they log into the NetScreen-Security Manager system

- To authenticate RAS users in VPNs

For step-by-step instructions on configuring a RADIUS authentication server to authenticate administrators and users, see the NetScreen-Security Manager Online Help topic “Editing the Domain Contact.”

Domain Versioning

Each time you update a device configuration on a security device using NetScreen-Security Manager, a new version of the device domain is automatically created. NetScreen-Security Manager archives the previous domain version and stores it on the GUI Server. You can view these previous versions to identify changes in the domain.

To view a previous version of a domain, click Tools > Select Domain Version, and select the domain version. Domain versions display according to their timestamp, which indicates the time and date a device configuration in the domain was last installed on a managed device. After you have selected domain, click OK; NetScreen-Security Manager displays the archived domain version as a read-only domain.

An archived domain version displays the modules (Device Manager, Security Policies, Log Investigator, and so on) that were saved during the versioning process. Because the versioning process saves only the modules that were changed, some modules might not appear. You cannot edit objects, policies, or other parameters for an archived domain version.
To return to the current domain version, click Tools > Select Domain Version, and select the most recent domain version.

NOTE: When upgrading to a new release of NetScreen-Security Manager, you will need to migrate your domain versions. During the upgrade process, the installer script prompts you to upgrade your domain versions. Because the number and size of the data in domain versions can grow to be quite large, it can take an extraordinary amount of time to migrate this data. If you choose not to migrate data about your versioned domains as part of the upgrade process, a tool is provided in the NetScreen-Security Manager utility package enabling you to migrate the data manually. For more information on migrating domain versions from previous releases of NetScreen-Security Manager, refer to the NetScreen-Security Manager Installer Guide.

EXAMPLE: CONFIGURING ROLE-BASED ADMINISTRATION
In this example, you configure a domain structure for an Internet Service Provider (ISP) with a co-location facility in New York that handles customers across four states. The company uses a two-letter state postal code combined with the customer name. Their goal is to manage all devices and policies from the co-location facility and provide read-only permission for customers to view log entries and generate reports. No VPNs are used.

To configure this domain structure, use the following process:

- Create the subdomains
- Create the subdomain administrators
- Create the read-only customer administrator
- Login as each administrator (for verification)

**Step 1: Create the Subdomains**
In this step, you create a subdomain for each company that uses the ISP.

1. Log in to the global domain as the superadmin.
2. From the Menu bar, select Tools > Manage Domains and Administrators.
3. Click the Subdomains tab, then click the Add icon to create a subdomain for the first customer. Configure the following four subdomains:
   - MA_company1
   - NH_company2
   - RI_company3
   - VT_company4
4. Click OK to save your changes.
Step 2: Create the Subdomain Administrator

In this step, you create a subdomain administrator with full permissions for the domain.

1. Using the domain menu (at the top of the navigation tree), select the first subdomain (MA_company1). NetScreen-Security Manager loads the subdomain.

2. From the Menu bar, click Tools > Manage Domains and Administrators.

3. In the Administrators tab, click the Add icon to create the primary administrator for this domain:
   - In the General Properties tab, enter a name, color, and contact information for the admin.
   - In the Authorization tab, leave the default authentication as Local and configure a password for the admin.
   - In the Permissions tab, click the Add icon, then configure the role as Domain Administrator (predefined) and the Domain as MA_company1.

4. Click OK to save your changes.

5. Repeat for each subdomain.

Step 3: Create the Viewing and Reporting Administrator

In this step, you create a custom role and admin account that permits the ISP customers to view log entries and generate reports for devices in their subdomain.

1. Using the domain menu (at the top of the navigation tree), select the first subdomain (MA_company1). NetScreen-Security Manager loads the subdomain.

2. From the Menu bar, click Tools > Manage Domains and Administrators.

3. In the Roles tab, click the Add icon to create a role that includes viewing and reporting permissions for this domain, as shown below:
4. Click OK to save your changes.
5. In the Administrators tab, click the Add icon to create the customer administrator for this domain:
   - In the General Properties tab, enter a name, color, and contact information for the admin.
   - In the Authorization tab, leave the default authentication as Local and configure a password for the admin.
   - In the Permissions tab, click the Add icon, then configure the role as Viewing & Reporting and the Domain as MA_company1.
6. Click OK to save your changes and return to the Administrators tab, which should display the following administrators:

Figure 11: Manage Administrators and Domains: Administrators Tab

7. Click OK to save your changes.

8. Repeat for each subdomain.

**Step 4: Verify Administrator Accounts**

In this step, you login as each administrator to verify their permissions (administrators must log in to the domain they were created in). Start a new instance of the NetScreen-Security Manager UI, then login as the following admins to test permissions.

- **Logging in as the Domain Administrator**—To login as the domain administrator, in the login screen, enter the subdomain/domain admin name (MA_company1/MA_Admin), the password, and GUI Server IP address. Click OK to login. The NetScreen-Security Manager navigation tree and main display area appear. Because the domain admin account has full permissions for the domain, the UI displays all modules and enables all functionality for the domain. However, the domain menu (at the top of the navigation tree) displays only the current domain, restricting the domain admin to that domain. Repeat for each subdomain and domain admin.

- **Logging in as the Customer Administrator.** To login as the customer admin, in the login screen, enter the subdomain/domain admin name (MA_company1/Customer_Admin), the password, and GUI Server IP address. Click OK to login. The NetScreen-Security Manager navigation tree and main display area appear. Because the customer admin account has permission only for viewing and report, the UI displays only the modules that are use for those permissions (note that Server Manager, Job Manager, and the Audit Log Viewer do not appear). Additionally, all Add, Edit, and Delete icons appear in gray, indicating that the admin cannot perform these tasks. Repeat for each subdomain and customer admin.
EXAMPLE: CONFIGURING AN IDP-ONLY ADMINISTRATOR

In this example, you (the super admin) create a custom role and IDP administrator who can only perform tasks that are specific to configuring and administering IDP on the standalone IDP device.

1. Log in to the global domain as the superadmin. From the Menu bar, select Tools > Manage Administrators and Domains.

2. Click the Roles tab, then click the Add icon to create a role called “IDP_Only”. Select tasks that are specific for IDP configuration and administration, such as:
   - Attack Update
   - Create/View/Edit/Delete Policies
   - Create/View/Edit/Delete Backdoor and IDP Rulebases
   - View Firewall Rulebases
   - Create/Edit/Delete Shared Objects and Groups

Select any other tasks that may be helpful for the IDP administrator; for example, you can select the options to view Jobs and view the System Status Monitor.

3. Click OK in the New Role dialog box to return to the Manage Administrators and Domains dialog box.

4. Click the Administrators tab, then click the Add icon to create an administrator called “IDP_Administrator”. The New Admin dialog box appears, with the General tab selected.

5. In the Name field, enter “IDP_Administrator”. You can enter contact information for the administrator.

6. Click the Authorization tab. Select the authorization method and the local password for the administrator.

7. Click the Permissions tab. Click the Add icon to select the role “IDP_Only” for this administrator.

8. Click OK to close the New Select Role and Domains dialog box. Click OK to close the New Admin dialog box. Click OK to close the Manage Administrators and Domains dialog box.

The administrator for the standalone IDP device can now log in to NetScreen-Security Manager as “IDP_Administrator”. Upon login, the NetScreen-Security Manager UI displays a limited navigation tree and menu options for this user. Note that the UI displays only the Security Policy and Object Manager options in the navigation tree and the Devices > Configuration options are not available for this user.
Part 2
Integrating

The chapters in Part 2 of the NetScreen-Security Manager 2005.3 Administrators Guide are designed to help you integrate new and existing network security devices into the management system, then configure and maintain those devices using the UI.

Part 2 contains the following chapters:

- Chapter 4 “Adding Devices” details how to add security devices to NetScreen-Security Manager. This chapter also describes how to use Rapid Deployment to quickly deploy devices in non-technical environments.

- Chapter 5 “Configuring Devices” details how to create a device configuration, including zones, interfaces, and routes. This chapter also describes how to use templates and groups to manage multiple devices more efficiently.

- Chapter 6 “Updating Devices” details how to use configuration summaries, update your device configurations, and use Job Manager to track the update progress.

- Chapter 7 “Managing Devices” details how to maintain device features, manage device images, and update AntiVirus and Deep Inspection files on the device.

After you have integrated your security devices into the management system and are familiar with the device configuration, updating, and management features in the UI, you are ready to begin building the Security Policies and VPNs that control your network traffic, as detailed in Part 3, “Managing” on page 439.
Chapter 4
Adding Devices

Security devices are the Juniper Networks device that you use to enable access to your network components and to protect your network against malicious traffic.

Juniper Networks NetScreen-Security Manager can manage all Juniper Networks security devices running Juniper Networks ScreenOS 5.x and ScreenOS 4.0.x (except 4.0.2). NetScreen-Security Manager can also manage vsys configurations, NSRP clusters, Vsys clusters, and extranet devices.

**NOTE:** The Juniper Networks NetScreen-5 device, Juniper Networks NetScreen-10 device, and Juniper Networks NetScreen-1000 device are not supported.

Before you can manage a device with NetScreen-Security Manager, you must add the device to the management system. NetScreen-Security Manager supports adding individual devices or many devices one at a time.

Use Rapid Deployment (RD) to quickly add devices in non-technical environments with no staging requirements.

The following sections are in this chapter:

- About Device Creation
- Before You Begin
- Importing Devices
- Modeling Devices
- Using Rapid Deployment
- Adding Other Device Types
- Adding Many Devices
About Device Creation

Before NetScreen-Security Manager can manage devices, you must first add those devices to the management system using the UI. To add a device, you create an object in the UI that represents the physical device, then create a connection between the UI object and the physical device so that their information is linked. When you make a change to the UI device object, you can push that information to the real device so the two remain in sync. You can add a single device at a time or add multiple devices all at once.

**NOTE:** The connection between a managed device and the NetScreen-Security Manager Device Server must be at least 28.8 kbps.

You can add the following types of devices:

- **Security devices**—A security device or system (such as a NetScreen-5GT device, a NetScreen-500 device, ISG 2000 device, or ISG 1000 device) is a device that manages firewall, VPN, and/or IDP activities on your network. The “Importing Devices” and “Modeling Devices” sections of this chapter detail how to add an existing or new security device into NetScreen-Security Manager. For details on adding many devices or systems at one time, see “Adding Many Devices” on page 119.

- **Vsyst devices**—A vsys is a virtual device that exists within a physical security device. For details on adding vsys devices, see Adding Vsyst Devices on page 111.

- **Clusters**—A cluster is two security devices joined together in a high availability configuration to ensure continued network uptime. For details on adding clusters, see “Adding a Cluster” on page 115.

- **Vsyst clusters**—A Vsyst cluster device is a vsys device that has a cluster as its root device. For details on adding Vsyst clusters and Vsyst devices, see “Adding a Vsyst Cluster and Vsyst Cluster Members” on page 116.

- **Extranet devices**—An extranet device is a device that is not a security device. For details on adding extranet devices, see “Adding an Extranet Device” on page 115.

Before adding any device type, you must determine the device status. After adding the device, you must verify the device configuration.

**Determine Device Status**

How you add your devices to the management system depends on the network status of the device:
Import deployed devices—Deployed devices are the devices you are currently using in your existing network. These devices run 5.x or earlier version of ScreenOS, and have already been configured with an IP address, zones, and other basic network information. For deployed devices, you can import the existing device configuration information into NetScreen-Security Manager.

Model undeployed devices—Undeployed devices are devices that you are not currently using in your network, and typically do not have IP addresses, zones, or other basic network information. For undeployed devices, you can model a new device configuration, then install that configuration on the device.

To help you add a device, the UI contains an Add Device wizard that walks you through each step of the device creation process. The Add Device wizard prompts you for specific device information like device type, IP address, and device admin name, then uses that information to enable the physical device to connect to the Device Server.

After the physical device connects, it is considered a managed device, meaning it is now under the control of the NetScreen-Security Manager.

Verify Device Configuration

For managed devices that use imported device configurations, you should verify that all device information was imported correctly. To identify any discrepancies, you can generate a summary of the differences between the physical device configuration and the NetScreen-Security Manager device configuration (this summary is known as a Delta Configuration Summary). It’s also a good idea to check your imported Security Policies, objects, and VPNs to become familiar with how the NetScreen-Security Manager UI displays them.

For managed devices that use modeled device configurations, you should verify that all device information was pushed to the physical device correctly. To identify discrepancies, generate a summary of the device configuration that is running on the physical device (this summary is known as a Get Running Config Summary).

Managing the Device

After successfully adding a device, you can begin managing its device configuration, objects, and Security Policies in the UI. You can also begin viewing traffic log entries for your device in the Log Viewer, administrative log entries in the Audit Log Viewer, and monitoring the status of your devices in Realtime Monitor.
You can also delete devices from NetScreen-Security Manager, and re-import them if necessary. Deleting a device removes all device configuration information from the management system, but might be the best solution if you need to perform extensive troubleshooting and/or reconfigure the device locally. After you have made the necessary changes locally, you can then re-import that device into the NetScreen-Security Manager system. However, during re-import, NetScreen-Security Manager imports all device configuration data—not just the data that was changed; any changes that exist in the modeled configuration are lost during re-import. Additionally, after re-importing a device configuration, you must reassign the imported policy to the device.

If you delete a device that was added using Rapid Deployment (described on page 104), you must also re-create the configlet and install it again on the device.

**Before You Begin**

Before adding a device to NetScreen-Security Manager, decide the following:

- Will you import or model the device?
- Will the device reside in the global domain or a subdomain?
- Will you be adding one or many devices?

Additionally, you should collect the following information about the device:

- ScreenOS version running on the device
- Port Mode used by the device

The following sections provide details to help you make device add decisions and determine device information.

**Importing vs. Modeling**

You must decide if you want to import or model your devices in NetScreen-Security Manager.

**Importing Device Configurations**

If you are currently using security devices in your existing network, you can add these devices into NetScreen-Security Manager and import their configurations. Using the Add Device Wizard, you configure a connection between the management system and the physical device, then import all device parameters, policies, objects, VPNs, and so on.

After you have imported several devices, you can start using system-level management features, such as the policy merge tool (merge several device Security Policies into a single, efficient policy that is easy to maintain), device groups (group devices by function, location, or platform to make updating easier), and the VPN Manager (create VPNs across multiple devices quickly).
Importing and Templates

If you assign a template to a device before connecting to and importing the device, later changes to the template will change values on the device. If you assign a template to a device after importing it, changes to the template will not change set values on the device unless you specifically have the template override the existing values.

Modeling Device Configurations

For new or undeployed security devices, you can add and configure the device in NetScreen-Security Manager, then activate the configuration when you are ready to deploy the physical device on your network.

Before connecting to the device, create a device (using the Add Device Wizard) that represents the ScreenOS platform and security device type of the actual, physical device. Then, model the device configuration in the NetScreen-Security Manager UI. Configure all device features—zones, interfaces, virtual routers, policies, logging features. Finally, activate the device (using the Activate Device Wizard) by configuring a connection between the management system and the physical device, then update the modeled configuration to the device.

To quickly configure multiple devices, use templates (re-usable, custom device settings such as DNS settings, PKI settings, and so on) and objects (re-usable, custom objects such as NAT objects, CA certificates, and Address objects). For large deployments that involve multiple devices in non-technical environments, use Rapid Deployment (RD) to bring new security devices under NetScreen-Security Manager management for initial configuration.

Device Add Process

Although the Add Device Wizard and Activate Device Wizard automatically handle many of the tasks involved in adding a device to the management system, you might need to manually perform some steps after using a wizard to complete the device add process.

The amount of manual involvement when adding a device to NetScreen-Security Manager depends on several factors, such as if you are importing a deployed device, activating a modeled device, the version of ScreenOS the device is running, and the type of IP address (static or dynamic) the device uses to connect to the management system. Figure 12 details the different device add processes and required manual steps for adding each type of security device and ScreenOS version.
Selecting the Domain

Determine the domain in which you want to place the device. A domain is a logical grouping of devices, device Security Policies, and device access privileges. NetScreen-Security Manager includes a global domain by default; you can also create additional domains, called subdomains, that exist within the global domain. Before you add the device, you must select the domain that contains the device; after the device is created, it appears only in that domain and must be managed from that domain.

When you log in to the UI for the first time after installing the management system, NetScreen-Security Manager loads the global domain by default, and the Device Manager does not contain any devices. To begin adding devices, ensure that you are in the domain you want to add the device to:

- Add device to the global domain—Ensure that you are in the global domain and begin the device creation process.
Add device to an existing subdomain—From the domain menu at the top of the
navigation tree, select the subdomain you want to add the device to and then
begin the device creation process. The domain menu displays only the domains
you have access to.

Add device to a new subdomain—You must first create the new subdomain in
NetScreen-Security Manager before adding devices to that subdomain. For
details on creating new subdomains, see Chapter 3, Configuring Role-Based
Administration. After you have created the subdomain, select it from the
domain menu and begin the device creation process.

After you have created subdomains, you can load a specific subdomain
automatically when you log in to the UI. You must have access to that
subdomain, and permissions to create, edit, and view devices in that
subdomain.

Domain selection is critical when using VPNs. You can create VPNs only between
devices within the same domain. If you need to add a device to a VPN in a different
domain, add the device as an extranet device in the domain that contains the VPN,
then add the extranet device to the VPN (as shown in Figure 13).

Figure 13: Connecting Devices from Different Domains in VPNs

Adding Single or Multiple Devices

Determine if you want to add devices to NetScreen-Security Manager individually or
add many devices all at one time (security devices and systems only). The adding
process for a single device is different than the process for adding multiple devices.

When adding a single security device, you use the Add Device Wizard to create the
device object in NetScreen-Security Manager. To activate a modeled device and/or
create a configlet, you use the Activate Device Wizard. You can import or model
device configurations from a device running ScreenOS 4.0.x or 5.x.

When adding many devices, you first create a .csv file that defines all required and
optional parameters for each device, then use the Add Many Device Wizard to
create a device object for each device in NetScreen-Security Manager. To activate
modeled devices and create configlets for each device, you use the Activate Many
Device Wizard.
You can use the Add Many Devices wizard for the following tasks:

- Import many ScreenOS 4.0.x and 5.x devices at one time.
- Model many ScreenOS 5.x devices at one time.
- Model, create configlets for, and activate multiple ScreenOS 5.x devices at one time for use with Rapid Deployment.

Additionally, you can use the Activate Many Devices wizard to create configlets for and activate multiple ScreenOS 5.x devices at one time for use with Rapid Deployment. However, you cannot activate multiple ScreenOS 5.x devices without creating configlets. For details, see “Adding Many Devices” on page 119.

**Determining ScreenOS Version**

During the Add Device or Add Many Devices process, you might need to specify the version of ScreenOS that is running on the device or devices:

- For devices that use a static IP address, you do not need to specify the ScreenOS version. NetScreen-Security Manager automatically detects this information during the add process.

- For undeployed devices or for devices that use a dynamically-assigned IP address, you must specify the ScreenOS version of the device. NetScreen-Security Manager validates the version during the model or add process.

Additionally, ensure that the devices you are adding to NetScreen-Security Manager are running a supported version of ScreenOS. NetScreen-Security Manager supports devices running 4.0.x or newer versions of ScreenOS; if you are not running a supported version, you must upgrade your devices before adding them into the management system. Contact Juniper Networks customer support for details.

**Determining Port Mode**

For some security devices, you can select a port mode during the model or add device process. The port mode automatically sets different port, interface, and zone bindings for the device. Port refers to a physical interface on the back of the physical security device; ports are referenced by their labels: Untrusted, 1-4, Console, or Modem. Interface refers to a logical interface that you can configure after you have added the device to the management system. You can bind each port to only one interface, but you can bind multiple ports to a single interface. For details, see “Configuring Interfaces” on page 222.

On the NetScreen-5XT and NetScreen-5GT devices, you can configure one of the following port modes:

- Trust-Untrust Port Mode
- Home-Work Port Mode
- Dual-Untrust Port Mode
- Combined Port Mode
- Trust-Untrust-DMZ Port Mode
- DMZ-Dual-Untrust Port Mode

**Trust-Untrust Port Mode**

Trust-Untrust mode is the default port mode. See Figure 14 for port, interface, and zone bindings.

**Figure 14: Trust-Untrust Port Mode Bindings**

- Binds the Untrusted Ethernet port to the Untrust interface, which is bound to the Untrust security zone
- Binds the Modem port to the serial interface, which you can bind as a backup interface to the Untrust security zone
- Binds the Ethernet ports 1 through 4 to the Trust interface, which is bound to the Trust security zone

**Home-Work Port Mode**

Home-Work mode binds interfaces to the Untrust security zone and to Home and Work security zones. The Home and Work zones enable you to segregate users and resources in each zone. In this mode, default policies permit traffic flow and connections from the Work zone to the Home zone, but do not permit traffic from the Home zone to the Work zone. By default, there are no restrictions for traffic from the Home zone to the Untrust zone. See Figure 15 for port, interface, and zone bindings.
Figure 15: Home-Work Port Mode Bindings

The ethernet3 interface is the primary interface to the Untrust zone. You can bind the serial interface (shown in gray) as a backup interface to the Untrust zone.

- Binds the Ethernet ports 1 and 2 to the ethernet1 interface, which is bound to the Work security zone
- Binds the Ethernet ports 3 and 4 to the ethernet2 interface, which is bound to the Home security zone
- Binds the Untrusted Ethernet port to the ethernet3 interface, which is bound to the Untrust security zone
- Binds the Modem port to the serial interface, which you can bind as a backup interface to the Untrust security zone

Dual-Untrust Port Mode

Dual Untrust mode binds two interfaces, a primary and a backup, to the Untrust security zone. The primary interface is used to pass traffic to and from the Untrust zone, while the backup interface is used only when there is a failure on the primary interface.

See Figure 16 for port, interface, and zone bindings.

Figure 16: Dual-Untrust Port Mode Bindings

The ethernet3 interface is the primary interface to the Untrust zone. The ethernet2 interface (shown in gray) is a backup interface to the Untrust zone.

- Binds the Untrusted Ethernet port to the ethernet3 interface, which is bound to the Untrust security zone
Binds Ethernet port 4 to the ethernet2 interface, which is bound as a backup interface to the Untrust security zone (the ethernet3 interface is the primary interface to the Untrust security zone).

Binds the Ethernet ports 1, 2, and 3 to the ethernet1 interface, which is bound to the Trust security zone.

NOTE: The serial interface is not available in Combined port mode.

**Combined Port Mode**

Combined mode enables both primary and backup interfaces to the Internet and the segregation of users and resources in Work and Home zones.

NOTE: For the NetScreen-5XT, the Combined port mode is supported only on the NetScreen-5XT Elite (unrestricted users) platform.

See Figure 17 for port, interface, and zone bindings.

**Figure 17: Combined Port Mode Bindings**

The ethernet4 interface is the primary interface to the Untrust zone. The ethernet3 interface (shown in gray) is the backup interface to the Untrust zone.

- Binds the Untrusted Ethernet port to the ethernet4 interface, which is bound to the Untrust zone
- Binds Ethernet port 4 to the ethernet3 interface, which is bound as a backup interface to the Untrust zone (the ethernet4 interface is the primary interface to the Untrust security zone)
- Binds the Ethernet ports 3 and 2 to the ethernet2 interface, which is bound to the Home zone
- Binds Ethernet port 1 to the ethernet1 interface, which is bound to the Work zone

NOTE: The serial interface is not available in Combined port mode.
Trust-Untrust-DMZ Port Mode

Trust/Untrust/DMZ mode binds interfaces to the Untrust, Trust and DMZ security zones, enabling you to segregate web, email or other application servers from the internal network.

NOTE: The Trust/Untrust/DMZ port mode is supported only on the NetScreen-5GT Extended platform.

See Figure 18 for port, interface, and zone bindings.

Figure 18: Trust-Untrust-DMZ Port Mode Bindings

- Binds the Ethernet ports 1 and 2 to the ethernet1 interface, which is bound to the Trust security zone
- Binds the Ethernet ports 3 and 4 to the ethernet2 interface, which is bound to the DMZ security zone
- Binds the Untrusted Ethernet port to the ethernet3 interface, which is bound to the Untrust security zone
- Binds the Modem port to the serial interface, which you can bind as a backup interface to the Untrust security zone.

DMZ-Dual-Untrust Port Mode

DMZ/Dual Untrust mode binds interfaces to the Untrust, Trust, and DMZ security zones, enabling you to pass traffic simultaneously from the internal network.

NOTE: The DMZ/Dual Untrust port mode is supported only on the NetScreen-5GT Extended platform, with ScreenOS 5.1 and higher.

See Figure 19 for port, interface, and zone bindings.
Before You Begin

Chapter 4: Adding Devices

Figure 19: DMZ Dual Untrust Port Mode

The ethernet3 and ethernet4 interfaces are active simultaneously. In this diagram, the two interfaces are bound to the Untrust zone to allow for load balancing.

- Binds the Ethernet ports 1 and 2 to the ethernet1 interface, which is bound to the Trust security zone
- Binds the Ethernet port 3 to the ethernet2 interface, which is bound to the DMZ security zone
- Binds the Ethernet port 4 to the ethernet3 interface, which is bound to the Untrust security zone
- Binds the Untrust Ethernet port to the ethernet4 interface, which is bound to the Untrust security zone

NOTE: The serial interface is not available in DMZ-Dual-Untrust port mode.

To enable failover instead of passing traffic simultaneously, you can configure the failover settings in the device configuration after you have added the device to the management system. For details, see “Configuring Interface Failover” on page 286.

Port Mode Summary

The following tables summarizes the port, interface, and zone bindings provided by the ScreenOS port modes:

Table 7: Security Device Port Mode Summary (Part 1)

<table>
<thead>
<tr>
<th>Porta</th>
<th>Trust-Untrust Modeb</th>
<th>Home-Work Mode</th>
<th>Dual Untrust Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Interface</td>
<td>Zone</td>
<td>Interface</td>
</tr>
<tr>
<td>Untrusted</td>
<td>Untrust</td>
<td>Untrust</td>
<td>ethernet3</td>
</tr>
<tr>
<td>1</td>
<td>Trust</td>
<td>Trust</td>
<td>ethernet1</td>
</tr>
<tr>
<td>2</td>
<td>Trust</td>
<td>Trust</td>
<td>ethernet1</td>
</tr>
<tr>
<td>3</td>
<td>Trust</td>
<td>Trust</td>
<td>ethernet1</td>
</tr>
<tr>
<td>4</td>
<td>Trust</td>
<td>Trust</td>
<td>ethernet2</td>
</tr>
<tr>
<td>Modem</td>
<td>serial</td>
<td>Null</td>
<td>serial</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>N/A</td>
</tr>
</tbody>
</table>

a. As labeled on the Juniper Networks security device chassis.
b. Default port modes
Changing the Port Mode

After you have added a device, you **cannot** change the port mode setting using NetScreen-Security Manager. You must delete the device from the management system, change the port mode using the WebUI or CLI, then re-add the device using the Add Device or Add Many Devices wizard.

When changing the port mode on the device, be aware that:

- Changing the port mode removes any existing configurations on the security device and requires a system reset.
- Issuing the `unset all` CLI command does not affect the port mode setting on the security device.

Importing Devices

NetScreen-Security Manager can import device configurations from devices running ScreenOS 5.x or earlier. The process differs slightly for 5.x devices and 4.0.x devices.

When importing ScreenOS 4.0.x devices, the management system connects to the device and imports the CLI command statements that detail the device configuration. The connection is secured using a standard encryption method; multiple, temporary connections between the management system and device are possible.
When importing ScreenOS 5.x devices, the management system connects to the device and imports Data Model (DM) information that details the device configuration. The connection is secured using Secure Server Protocol (SSP), a proprietary encryption method; an always-on connection exists between the management system and device.

Adding a single deployed device to NetScreen-Security Manager is a three stage process:

1. Add the device.
2. Import the configuration.
3. Verify the imported configuration.

In some cases, you may need to configure NACN or other features on the physical device to enable the device to connect to NetScreen-Security Manager.

For details on adding multiple devices at one time, see “Adding Many Devices” on page 119.

Requirements
To import a single device:

- The physical device must have Telnet or SSH enabled.
- You must have the device connection information (IP address, connection method) and device admin name and password available.

NOTE: All passwords handled by NetScreen-Security Manager are case-sensitive.

- The device must be staged (physically connected to your network with access to network resources).
- The device must have at least one interface that has an IP address. Devices that use dynamically assigned IP address must also support NACN.
The device must be operating in the desired mode. You cannot change the operational mode after importing the device into NetScreen-Security Manager.

**NOTE:** After importing a device configuration, log entries from that device begin to appear in the Log Viewer. However, until you update the device from NetScreen-Security Manager, the following log fields display 0 (or unknown):

- For 5.x devices: domain, domain version, rulebase, policy, rule number.
- For 4.0.x devices: domain, domain version, rulebase, policy, rule number, from zone, to zone, action.

After you update the imported device configuration using NetScreen-Security Manager, the appropriate values are displayed for log entries from the device.

### Adding Devices with Static IP Addresses

A static IP address is an IP address that does not change.

**ScreenOS 4.0.x Devices**

To import a ScreenOS 4.0.x device with a known IP address:

1. From the domain menu, select the domain in which to import the device.
2. In Device Manager, click the Add icon and select Device. The Add Device wizard appears.
   - Enter a name and select a color to represent the device in the UI.
   - Select Device is Reachable (default).
3. Click Next to display the Specify Connection Settings dialog box. Enter the connection information:
   - Enter the IP Address of the security device.
   - Enter the username of the device admin.
   - Enter the password for the device admin.

**NOTE:** All passwords handled by NetScreen-Security Manager are case-sensitive.

- Select the connection method (Telnet, SSH version 1) and the port number for the selected service.
  
  If you selected Telnet, click Next and go to step 4.

  If you selected an SSH version, click Next to display The Verify Device Authenticity dialog box. The device wizard displays the RSA Key Fingerprint information; to prevent man-in-the-middle attacks, you should verify the fingerprint using an out-of-band method.
4. The wizard displays the autodetected device information. Verify that the device type, ScreenOS version, and the device serial number are correct, then select the Device Server connection:

- Use the default settings to configure the device to connect to the NetScreen-Security Manager Device Server IP address and port.
- Use a MIP to configure the device to connect to the NetScreen-Security Manager Device Server through a mapped IP address and port.

Click Next.

5. Select Enable Logging to enable NetScreen-Security Manager to collect log entries from the device.

6. To configure NACN, click the Add icon to display the Arbitrator dialog box. The Add Device Wizard automatically completes the PM Cert Subject Name, Device Server Address, and NACN Registering Port for you. Configure the remaining fields:

- For Interface Monitored, select the untrust interface.
- For NACN Password, enter the password that authenticates NACN communication between the device and the management system.

Click OK to add the NACN Arbitrator.

Click Show Device Commands to display a list of CLI commands. Copy and paste these commands into a text file.

Send the commands to the device administrator. The device admin must make a telnet connection to the physical device, paste the commands, and execute them to enable NACN on the device.

The device cannot connect to NetScreen-Security Manager until these commands are executed on the physical device.

7. Click Finish to complete the Add Device wizard. The wizard automatically imports the device configuration. After the import is complete, double-click the device to view the imported configuration.

To check the device configuration status, mouseover the device in Device Manager (you can also check configuration status in Device Monitor). The device status displays as Managed, indicating that the device has connected and the management system has successfully imported the device configuration.
ScreenOS 5.x Devices

To import a ScreenOS 5.x device with a known IP address:

1. From the domain menu, select the domain in which to import the device.
2. In Device Manager, click the Add icon and select Device. The Add Device wizard appears.
   - Enter a name and select a color to represent the device in the UI.
   - Select Device is Reachable (default).
3. Click Next to display the Specify Connection Settings dialog box. Enter the connection information:
   - Enter the IP Address of the security device.
   - Enter the username of the device admin.
   - Enter the password for the device admin.
4. The wizard displays the autodetected device information. Verify that the device type, ScreenOS version, and the device serial number are correct.
5. Click Finish to complete the Add Device wizard. The new device appears in the Device Manager list.
6. If you can access the device paste these commands into the device yourself and execute them. Otherwise, send the text file that contains the commands generated in the previous step to the device administrator, who opens a telnet connection to the physical device, pastes the commands, and executes them to enable NetScreen-Security Manager management on the device.
7. To check the device configuration status, mouseover the device in Device Manager (you can also check configuration status in Device Monitor):
   - Before the device connects, the status displays **Waiting for 1st connect**, indicating that the management system is waiting for the device to connect. (This event occurs quickly and might not display.)
After the device connects, the status displays **Import Needed**, indicating that the device has connected but the management system has not imported the device configuration yet.

### 8. Importing Devices

After the device connects, the status displays **Import Needed**, indicating that the device has connected but the management system has not imported the device configuration yet.

8. Import the device configuration by right-clicking the device and selecting **Import Device**. The Job Information box appears and displays the job type and status for the import; when the job status displays successful completion, click **Close**.

After the import is complete, double-click the device in Device Manager to view the imported configuration.

**NOTE:** After importing a NetScreen-5GT that uses extended port mode, NetScreen-Security Manager displays the modes as “ns5GT-Trust-Untrust-DMZ” and sets the license mode to extended.

To check the device configuration status, mouseover the device in Device Manager (you can also check configuration status in Device Monitor). The device status displays as **Managed**, indicating that the device has connected and the management system has successfully imported the device configuration.

### Adding Devices with Dynamic IP Addresses

A dynamic IP address is an IP address that changes. To add a ScreenOS device that uses a dynamic IP address, the device must support NACN.

**ScreenOS 4.0.x Devices**

To import a ScreenOS 4.0.x device with an unknown IP address:

1. From the domain menu, select the domain in which you want to import the device.

2. In Device Manager, click the **Add** icon and select **Device**. The Add Device wizard appears.

   - Enter a name and select a color to represent the device in the UI.
   - Select **Device is not Reachable**.

3. Click **Next** to display the New Device dialog box:

   - Enter the device type and specify the ScreenOS version that is running on the device.

   - If desired, enable **Transparent Mode**.

   - Select the Device Server connection: Use the default settings to configure the device to connect to the NetScreen-Security Manager Device Server IP address and port. Use a MIP to configure the device to connect to the NetScreen-Security Manager Device Server through a mapped IP address and port.
4. Click Next to display the Configure NACN and Global-PRO Logging dialog box.
   - Enter the Serial Number of the device.
   - Enable Global-PRO logging to enable NetScreen-Security Manager to collect log entries from the device.
   - Enter the username and password of the device admin.

   NOTE: All passwords handled by NetScreen-Security Manager are case-sensitive.

5. To configure NACN, click the Add icon to display the Arbitrator dialog box. The Add Device Wizard automatically completes the PM Cert Subject Name, Device Server Address, and NACN Registering Port for you.
   - For Interface Monitored, select the untrust interface.
   - For NACN Password, enter the password that authenticates NACN communication between the device and the management system.

   NOTE: All passwords handled by NetScreen-Security Manager are case-sensitive.

   - Click OK to add the NACN Arbitrator.
   - Click Show Device Commands to display a list of CLI commands. Copy and paste these commands into a text file.
   - Send the commands to the device administrator. The device admin must make a telnet connection to the physical device, paste the commands, and execute them to enable NACN on the device.

   NOTE: The device admin can also use a console connection to execute the commands on the physical device. However, the commands must be entered three at a time to ensure that the device receives all commands.

   The device cannot connect to NetScreen-Security Manager until these commands are executed on the physical device.

6. Click Finish to complete the Add Device wizard. The new device appears in the Device Manager list.

7. To check the device configuration status, mouseover the device in Device Manager (you can also check configuration status in Device Monitor):
   - Before the device connects, the status displays Waiting for 1st connect, indicating that the management system is waiting for the device to connect. (This event occurs very quickly and might not display.)
   - After the device connects, the status displays Import Needed, indicating that the device has connected but the management system has not imported the device configuration yet.
8. Import the device configuration by right-clicking the device and selecting Import Device. The Job Information box appears and displays the job type and status for the import; when the job status displays successful completion, click Close.

After the import is complete, double-click the device to view the imported configuration.

To check the device configuration status, mouseover the device in Device Manager (you can also check configuration status in Device Monitor). The device status displays as Managed, indicating that the device has connected and the management system has successfully imported the device configuration.

**ScreenOS 5.x Devices**

To import a ScreenOS 5.x device with an unknown IP address:

1. From the domain menu, select the domain in which you want to import the device.

2. In Device Manager, click the Add icon and select Device. The Add Device wizard appears.
   - Enter a name and select a color to represent the device in the UI.
   - Select Device is not Reachable.
   - Select the Device Server connection: Use the default settings to configure the device to connect to the NetScreen-Security Manager Device Server IP address and port. Use a MIP to configure the device to connect to the NetScreen-Security Manager Device Server through a mapped IP address and port.

3. Click Next. Enter the device type and specify the ScreenOS version that is running on the device. If desired, enable Transparent Mode.

4. Select the license key model for the device. Available selections depend on the type of security device and can include: baseline, advanced, extended, plus, 10-user.

5. Click Next.
   - The wizard automatically enters the Unique External ID for the device. This ID number represents the device within the management system.
   - Specify the First Connection One Time Password (OTP) that authenticates the device.

**NOTE:** All passwords handled by NetScreen-Security Manager are case-sensitive.

- Click Show Device Commands to display a list of CLI commands. The commands enable management and set the management IP address to the Device Server IP address, enable the Management Agent, set the Unique External ID, and set the device OTP.
- Copy and paste these commands into a text file,
- Click Finish to complete the Add Device wizard. The new device appears in the Device Manager list.

6. Add the commands to the console of the device. Send the commands to the device administrator. The device admin must make a telnet connection to the physical device, paste the commands, and execute them to enable NetScreen-Security Manager management on the device.

7. To check the device configuration status, mouseover the device in Device Manager (you can also check configuration status in Device Monitor):
   - Before the device connects, the status displays Waiting for 1st connect, indicating that the management system is waiting for the device to connect. (This event occurs very quickly and might not display.)
   - After the device connects, the status displays Import Needed, indicating that the device has connected but the management system has not imported the device configuration yet.

8. Import the device configuration by right-clicking the device and selecting Import Device. The Job Information box appears and displays the job type and status for the import; when the job status displays successful completion, click Close.

   After the import is complete, double-click the device to view the imported configuration.

   **NOTE:** After importing a NetScreen-5GT that uses extended port mode, NetScreen-Security Manager displays the modes as “ns5GT-Trust-Untrust-DMZ” and sets the license mode to extended.

   To check the device configuration status, mouseover the device in Device Manager (you can also check configuration status in Device Monitor). The device status displays as Managed, indicating that the device has connected and the management system has successfully imported the device configuration.

**Verifying Imported Device Configurations**

After importing a device, you should verify that all device information was imported as you expected.

**Using Device Monitor**

The Device Monitor tracks the status of individual devices, systems, and their processes. After you import a device, you should check the status of that device in Device Monitor, located in Realtime Monitor.

The imported device should display a configured status of Managed and a Connection status of UP, indicating that the device has connected and the management system has successfully imported the device configuration.
Using Device Manager

In the security device tree, ensure that the device exists, then open the device configuration and check the following values:

- Ensure that the imported device serial number matches the serial number on the physical device.
- Ensure that the imported device IP address matches the IP address for the physical device.
- Ensure that imported device administrator name and password are correct for the physical device.

**NOTE:** All passwords handled by NetScreen-Security Manager are case-sensitive.

- Ensure that interfaces on the imported device are correct for the physical device.

**NOTE:** When importing an NetScreen-500, 5000 series, or ISG series security device, you must manually configure the network module (slot) before the imported physical interfaces appear in the NetScreen-Security Manager UI. For details on defining the ethernet card and slot, see “Configuring the Network Module” on page 167.

- Browse the device configuration tree and ensure that the management system successfully imported all device configuration information, including zones, virtual routers, and routes.

Using Job Manager

Job Manager tracks the status of major administrative tasks, like importing or updating a device. After you import a device, it’s a good idea to view the report for the import task to ensure that the management system imported the device configuration as you expected.

**NOTE:** Job Manager configuration summaries and job information details do not display passwords in the list of CLI commands for administrators that do not have the assigned activity “View Device Passwords”. By default, only the super administrator has this assigned activity.

Job Manager also tracks the status of configuration summaries, described below.

Using Configuration Summaries

NetScreen-Security Manager provides three configuration summaries to help you manage device configurations and prevent accidental misconfiguration. You should use configuration summaries after you import a device to ensure that the management system imported the physical device configuration as you expected.
Configuration summaries help with ongoing device maintenance, too, particularly for devices on which a local device administrator has been troubleshooting using CLI commands or the WebUI. Because the UI device configuration can overwrite the physical device configuration, you should **always** confirm the commands that are sent to the device.

### Config Summary

A configuration summary shows you the exact CLI commands that will be sent to the managed device during the next device update. To get a Configuration Summary, from the menu bar click Devices > Configuration > Summarize Config to display a list of security devices to which you have access. Select the device you just imported and click OK. NetScreen-Security Manager analyzes the UI device configuration and generates a summary report that lists the CLI commands to send to the physical device during the next device update.

For a just-imported device, the config summary report should display the device configuration that matches the configuration currently running on the physical device.

### Delta Configuration Summary

A delta configuration summary shows you the differences between the configuration you see in the NetScreen-Security Manager UI and the configuration on the physical device. To get a Delta Configuration Summary, from the menu bar, click Devices Configuration > Summarize Delta Config to display a list of security devices to which you have access. Select the device you just imported and click OK. NetScreen-Security Manager queries the physical device to obtain a list of all CLI commands used in the device configuration, compares that list with the UI device configuration, and generates a summary report of all differences, or deltas discovered.

For a just-imported device, the delta config summary should display minimal deltas, meaning that very few differences exist between the configuration on the physical device and the configuration in the UI. NetScreen-Security Manager automatically imports your VPNs and displays the VPN policies; however, NetScreen-Security Manager does not create VPN abstractions for your VPN policies.

### Get Running Config

A running configuration summary shows you the exact CLI commands that were used to create the current device configuration on the physical device. To get the Running Config summary, from the menu bar click Device > Configuration > Get Running Config to display a list of security devices to which you have access. Select the device you just imported and click OK. NetScreen-Security Manager queries the physical device to obtain a list of all CLI commands used in the device configuration and generates a summary report that lists those commands.

For a just-imported device, the get running config summary report should display the device configuration currently running on the physical device.
Modeling Devices

For undeployed devices, you can create a device configuration in NetScreen-Security Manager then install that device configuration on the physical device. For ScreenOS 5.x devices, you can use Rapid Deployment (RD) to quickly provision multiple devices in non-technical environments. See “Using Rapid Deployment” on page 104 for details.

Adding a single undeployed device to NetScreen-Security Manager is a four stage process:

1. Model device in the UI
2. Create device configuration
3. Activate device
4. Update device configuration

For details on modeling multiple devices at one time, see “Adding Many Devices” on page 119.

Requirements

To model a device, you must know the device type and ScreenOS version that is running on the device.

To activate a device:

- You must have the device connection information and device admin name and password.

**NOTE:** All passwords handled by NetScreen-Security Manager are case-sensitive.

- The device must be staged (physically connected to your network and can access network resources).
- The device must have at least one interface that has an IP address. Devices that use dynamically assigned IP address must also support NACN.

**Modeling a Device**

To add a device:

1. From the domain menu, select the domain in which you want to import the device.
2. In Device Manager, click the Add icon and select Device. The device wizard appears.
   - Enter a name and select a color to represent the device in the UI.
   - Select Model Device.
3. Click Next to display the New Device platform dialog box. Enter the device platform and OS version.

NOTE: When adding a NetScreen-5GT that uses extended port mode, select the device type “ns5GT-Trust-Untrust-DMZ”. NetScreen-Security Manager automatically sets the license mode to extended.

4. Select the license key model for the device. Available selections depend on the type of security device, and can include: baseline, advanced, extended, plus, 10-user.

5. Enable transparent mode, if desired.

NOTE: You cannot change the operational mode after the device has been modeled.

6. Click Finish to complete the add device wizard. The UI creates a corresponding device object that appears in the Device Manager list.

7. To check the device configuration status, mouseover the device in Device Manager (you can also check configuration status in Device Monitor). The status displays Modeled, indicating that the management system has modeled the device, but the device is not activated and has not connected.

Creating a Device Configuration

Because undeployed devices are devices that you are not currently using in your network, they might not have a pre-existing device configuration (IP addresses, zones, and interfaces) that is available for import. You can create a configuration for the device in NetScreen-Security Manager, then install that configuration on the device.

NOTE: When modeling an NetScreen-500, 5000 series, or ISG series security device, you must configure the network module (slot) before physical interfaces appear in the NetScreen-Security Manager UI. For details on defining the ethernet card and slot, see “Configuring the Network Module” on page 167.

Double-click the device object to display the device configuration and begin configuring the device as desired. For details on device configuration, see Chapter 5, “Configuring Devices”.

Activating a Device

After you have created a device configuration for the undeployed device, you are ready to activate the device and prompt it to connect to the management system. After that device has made contact with NetScreen-Security Manager, you can install the configuration you created on the device.

Devices with Static IP Addresses

A static IP address is an IP address that does not change.
**ScreenOS 4.0.x Devices**

To activate a ScreenOS 4.0.x device with a static IP address:

1. Check the device configuration status by holding your mouse cursor over the device in Device Manager (you can also check configuration status in Device Monitor). The device status should display **Modeled**, indicating that the management system is waiting for the device to be activated.

2. Right-click the device and select Activate Device to display the Activate Device wizard. Select Device Deployed and IP is Reachable.

3. Click Next to display the Specify Connection Settings dialog box. Enter the connection information:
   - Enter the IP Address of the security device.
   - Enter the device admin name and password.

4. The wizard displays the autodetected device information. Verify that the device type, ScreenOS version, and the device serial number are correct, then select the Device Server connection:
   - Use the default settings to configure the device to connect to the NetScreen-Security Manager Device Server IP address and port.
   - Use a single or multiple MIPs to configure the device to connect to the NetScreen-Security Manager Device Server through a mapped IP address and port.

5. Click Next. Select Enable Logging to enable NetScreen-Security Manager to collect log entries from the device.

6. To configure NACN, click the Add icon to display the Arbitrator dialog box. The Add Device Wizard automatically completes the PM Cert Subject Name, Device Server Address, and NACN Registering Port for you.
   - For Interface Monitored, select the untrust interface.

---

**NOTE:** All passwords handled by NetScreen-Security Manager are case-sensitive.
For NACN Password, enter the password that authenticates NACN communication between the device and the management system.

NOTE: All passwords handled by NetScreen-Security Manager are case-sensitive.

- Click OK to add the NACN Arbitrator.
- Click Show Device Commands to display a list of CLI commands. Copy and paste these commands into a text file.
- Send the commands to the device administrator. The device admin must make a telnet connection to the physical device, paste the commands, and execute them to enable NACN on the device.

NOTE: The device admin can also use a console connection to execute the commands on the physical device. However, the commands must be entered three at a time to ensure that the device receives all commands.

The device cannot connect to NetScreen-Security Manager until these commands are executed on the physical device.

7. Check the device configuration status by holding your mouse cursor over the device in Device Manager (you can also check configuration status in Device Monitor). When the device connects, the status displays **Update Needed**, indicating that the device has connected but the management system has not pushed the device configuration yet.

8. Update the device configuration by right-clicking the device and selecting Update Device. The Job Information box appears and displays the job type and status for the update; when the job status displays successful completion, click Close.

After update is complete, the device status displays as **Managed**, indicating that the device has connected and the management system has successfully pushed the device configuration.

**ScreenOS 5.x Devices**

To activate a ScreenOS 5.x device with a static IP address:

1. Check the device configuration status by holding your mouse cursor over the device in Device Manager (you can also check configuration status in Device Monitor). The device status should display **Modeled**, indicating that the management system is waiting for the device to connect.

2. Right-click the device and select Activate Device to display the Activate Device wizard. Select Device Deployed and IP is Reachable.

3. Click Next to display the Specify Connection Settings dialog box. Enter the connection information:
   - Enter the IP Address of the security device.
Enter the device admin name and password.

NOTE: All passwords handled by NetScreen-Security Manager are case-sensitive.

Select the connection method (Telnet, SSH version 1, SSH version 2) and the port number for the selected service.

If you selected Telnet, click Next and go to step 4.

If you selected an SSH version, click Next to display the Verify Device Authenticity dialog box. The device wizard displays the RSA Key Fingerprint information; to prevent man-in-the-middle attacks, you should verify the fingerprint using an out-of-band method.

4. Check the device configuration status by holding your mouse cursor over the device in Device Manager (you can also check configuration status in Device Monitor). When the device connects, the status displays Update Needed, indicating that the device has connected but the management system has not pushed the device configuration yet.

5. Update the device configuration by right-clicking the device and selecting Update Device. The Job Information box appears and displays the job type and status for the update; when the job status displays successful completion, click Close.

After update is complete, the device status displays as Managed, indicating that the device has connected and the management system has successfully pushed the device configuration.

Devices with Dynamic IP Addresses
A dynamic IP address is an IP address that changes. To add a ScreenOS device that uses a dynamic IP address, the device must support NACN.

ScreenOS 4.0.x Devices
To activate a ScreenOS 4.0.x device with an unknown IP address:

1. Check the device configuration status by holding your mouse cursor over the device in Device Manager (you can also check configuration status in Device Monitor). The device status should display Modeled, indicating that the management system is waiting for the device to connect.

2. Right-click the device and select Actions > Activate Device. The Activate Device wizard appears. Select Device Deployed but IP is Not Reachable.

3. Click Next to display the Configure NACN and Global-PRO Logging dialog box.

   - Enter the Serial Number of the device.
   - Enable Global-PRO logging to enable NetScreen-Security Manager to collect log entries from the device.
Enter the username and password of the device admin.

NOTE: All passwords handled by NetScreen-Security Manager are case-sensitive.

4. To configure NACN, click the Add icon to display the Arbitrator dialog box. The Add Device Wizard automatically completes the PM Cert Subject Name, Device Server Address, and NACN Registering Port for you.

- For Interface Monitored, select the untrust interface.
- For NACN Password, enter the password that authenticates NACN communication between the device and the management system.

NOTE: All passwords handled by NetScreen-Security Manager are case-sensitive.

- Click OK to add the NACN Arbitrator.
- Click Show Device Commands to display a list of CLI commands. Copy and paste these commands into a text file.
- Send the commands to the device administrator. The device admin must make a telnet connection to the physical device, paste the commands, and execute them to enable NACN on the device.

NOTE: The device admin can also use a console connection to execute the commands on the physical device. However, the commands must be entered three at a time to ensure that the device receives all commands.

The device cannot connect to NetScreen-Security Manager until these commands are executed on the physical device.

5. Click Finish to complete the Activate Device wizard.

6. Check the device configuration status by holding your mouse cursor over the device in Device Manager (you can also check configuration status in Device Monitor). When the device connects, the status displays **Update Needed**, indicating that the device has connected but the management system has not pushed the device configuration yet.

7. Update the device configuration by right-clicking the device and selecting Update Device. The Job Information box appears and displays the job type and status for the update; when the job status displays successful completion, click Close.

After the update is complete, the device status displays as **Managed**, indicating that the device has connected and the management system has successfully updated the device configuration.

**ScreenOS 5.x Devices**

To activate a ScreenOS 5.x device with an unknown IP address:
1. Check the device configuration status by holding your mouse cursor over the device in Device Manager (you can also check configuration status in Device Monitor). The device status should display **Modeled**, indicating that the management system is waiting for the device to connect.

2. Right-click the device and select Actions > Activate Device. The Activate Device wizard displays. Select Device Deployed but IP is Not Reachable.

3. Click Next. Select Initialize Device Manually. (For details on initializing with a configlet, see “Using Rapid Deployment” on page 104.)

4. Click Next.
   - Specify the First Connection One Time Password (OTP) that authenticates the device.

   NOTE: All passwords handled by NetScreen-Security Manager are case-sensitive.

   - Click Show Device Commands to display a list of CLI commands. The commands enable management and set the management IP address to the Device Server IP address, enable the Management Agent, set the Unique External ID, and set the device OTP.
   - Copy and paste these commands into a text file, then send the commands to the device administrator. The device admin must make a telnet connection to the physical device, paste the commands, and execute them to enable NetScreen-Security Manager management on the device.

   NOTE: The device admin can also use a console connection to execute the commands on the physical device. However, the commands must be entered three at a time to ensure that the device receives all commands.

5. Click Finish to complete the Activate Device wizard.

6. Check the device configuration status by holding your mouse cursor over the device in Device Manager (you can also check configuration status in Device Monitor). When the device connects, the status displays **Update Needed**, indicating that the device has connected but the management system has not pushed the device configuration yet.

7. Update the device configuration by right-clicking the device and selecting Update Device. The Job Information box appears and displays the job type and status for the update; when the job status displays successful completion, click Close.

After the updated is complete, the device status displays as **Managed**, indicating that the device has connected and the management system has successfully updated the device configuration.
Using Rapid Deployment

Rapid Deployment (RD) enables deployment of multiple security devices in a large networked environment with minimal user involvement. RD is designed to:

- Simplify the deployment of firewall devices in non-technical environments
- Minimal device staging or technical staff required at deployment site
- Enable secure and efficient deployment of a large number of firewalls
- Bring new security devices under NetScreen-Security Manager management for initial configuration

RD typically involves two people: The NetScreen-Security Manager administrator, who creates the necessary device configuration for the new firewall devices in the NetScreen-Security Manager management console, and the on-site admin, who enables the firewall device to contact NetScreen-Security Manager for configuration.

The **NetScreen-Security Manager administrator** works in the NetScreen-Security Manager UI. First, add a device to the UI, then creates a device configuration with specific or template-driven values. Next, enter the basic information that defines how a security device can contact your NetScreen-Security Manager Device Server and generate a small, static command file called a configlet. Save the configlet to a user-defined directory; using email, floppy disk, CD, or other out-of-band method, send the configlet file to the on-site admin that will be installing the configlet on the security device at its physical location. After the on-site admin installs the configlet and the device has successfully connected to the management system, you can install the modeled device configuration on the physical device.

The **On-Site administrator** works locally, at the physical device. At the security device, install the configlet on a locally-connected computer and run the Rapid Deployment Wizard. The RD wizard uses the information in the configlet to establish and authenticate a secure connection the NetScreen-Security Manager Device Server, enabling NetScreen-Security Manager to begin managing the device.

After the firewall device has connected to NetScreen-Security Manager, the NetScreen-Security Manager administrator can manage the device exactly like any other firewall in NetScreen-Security Manager.

**NOTE:** If you delete the security device from the NetScreen-Security Manager system then re-add the device, you must also re-create the configlet and install on the physical device.

Overview

The NetScreen-Security Manager administrator adds a single device with RD in three stages:

1. Creating the Configlet
2. Installing the Configlet (performed by the on-site admin)
3. Updating the Device Configuration
The sections below detail each stage. For details on modeling, creating configlets for, and activating multiple devices at one time, see “Adding Many Devices” on page 119.

Requirements

To use rapid deployment:

- The device must be running ScreenOS 5.x
- The device must use default factory settings.
- The device must be able to reach the Internet using a static IP address, a PPPoE- or PPPoA-assigned IP address, or DHCP-assigned IP address.
- The device must be modeled in NetScreen-Security Manager system. For details on modeling a device, see “Modeling a Device” on page 97

After you have modeled the device in the management system, you can begin tracking its status using the Device Monitor. Check the device configuration status by holding your mouse cursor over the device in Device Manager (you can also check configuration status in Device Monitor). The status should display Modeled, indicating that the management system has modeled the device, but the device is not activated and has not connected.

Creating the Configlet

After you have created a device configuration for the undeployed device, you are ready to activate the device and create the configlet.

1. Right-click the device and select Activate Device. The Activate Device wizard appears.
2. Select Device Deployed but IP is Not Reachable.
4. Click Next.
   - Specify the First Connection One Time Password that authenticates the device.

NOTE: All passwords handled by NetScreen-Security Manager are case-sensitive.

- The wizard automatically selects the interface on the device that will connect to the NetScreen-Security Manager management system. This interface is determined by the device platform and cannot be changed.
- Select the Device Server connection. Use the default settings to configure the device to connect to the NetScreen-Security Manager Device Server IP address and port. Use a MIP to configure the device to connect to the NetScreen-Security Manager Device Server through a mapped IP address and port.
5. Click Next.
   
a. Specify the connection setting on the device:

   - For devices with static IPs, you can pre-define the IP address, mask, and gateway OR ask the on-site admin to specify this information during configlet installation.
   
   - For devices that use DHCP, the configlet automatically handles IP assignment during installation.
   
   - For devices that use a PPPoE connection to the Internet, you can pre-define the user name and password OR ask the on-site admin to specify the user name and password during configlet installation.

   **NOTE:** All passwords handled by NetScreen-Security Manager are case-sensitive.

   - For devices that use a PPPoA connection to the Internet, you can pre-define the following ADSL parameters:

     - VPI/VCI Pair. The Virtual Path Identifier and Virtual Channel Identifier (VPI/VCI) identify the virtual circuit on the DSLAM.

     - Multiplexing Mode. Also known as the ATM encapsulation method, the multiplexing mode defines how the ADSL interface handles the multiple protocols on the virtual circuit. Your service provider must tell you the type of multiplexing used on the ADSL line:

       - Virtual Circuit (VC)-based multiplexing carries each protocol is carried over a separate ATM virtual circuit.

       - Logical Link Control (LLC) carries several protocols to be carried on the same ATM virtual circuit. This is the default option for the ADSL1 interface on the NetScreen-5GTADSL security device.

     - RFC1483 Protocol Mode. RFC 1483 describes methods of transporting bridged or routed protocol data units (PDUs) over AAL5 links:

       - Bridged PDUs do not require the overhead of IPSec processing, thus allowing more usable bandwidth to be available for data traffic. Because non-IPSec traffic is not secured at the IP packet layer, you should use this mode only with a private virtual circuit (the service provider assigns a static IP address for the ADSL interface).

       - Routed PDUs enable the NetScreen-5GT ADSL device to exchange routing information with another router through the ADSL interface.

     - ADSL Operating Mode. The operating mode defines the physical line attributes for the ADSL interface:
Auto Detect (default mode) enables the ADSL interface to automatically negotiate the operating mode with the service provider DSLAM.

ANSI T1.413 Issue 2 Mode

ITU G.992.1 Mode enables the ADSL interface to use the International Telecommunications Union (ITU) G.dmt standard, which supports minimum data rates of 6.144 Mbps downstream and 640 kbps upstream.

G.Lite Mode enables the ADSL interface to use the ITU 992.2 standard, which supports maximum data rates of 1.536 Mbps downstream and 512 kbps upstream.

Alternatively, you can prompt the on-site admin to specify these parameters during configlet installation.

If you don’t know the ISP environment or the environment has location-specific networking requirements, prompt the on-site admin to configure the ISP environment during configlet installation.

b. Specify the password for the configlet, or use the default device password (which is netscreen).

c. Specify Device User Names and passwords, or use the default admin name and passwords for the device.

d. Restrict the use of the configlet to the current device. If checked, the configlet can only be installed on a device with the specified serial number.

6. Click Next to display the decoded configlet. To see the encoded configlet, click the Raw Configlet tab. Click Save to save the configlet (configlet files automatically use the format .cfg).

NOTE: For security reasons, you cannot edit a configlet file directly. To make changes to the information in a configlet file, run the Activate Device wizard to re-generate the configlet.

7. Click Finish to complete the Activate Device wizard.

8. Send the configlet to the on-site admin using email, floppy disk, CD, or other out-of-band method.

To help the on-site admin through the configlet installation process, you should also send them the Rapid Deployment Getting Started Guide available on the Juniper Networks NetScreen-Security Manager Documentation CD. This guide provides step-by-step instructions for connecting a security device to the network, preparing the device to use a configlet, and installing and running the configlet.

The on-site admin must complete the configlet installation process and the device must successfully connect to the management system before you can update the device with the modeled configuration.
You can track the connection status of the device to determine when the device connects. Check the device configuration status by holding your mouse cursor over the device in Device Manager (you can also check configuration status in Device Monitor).

- Before the device connects, the status displays **Waiting for 1st Connect**, indicating that the management system has modeled and activated the device, but the device has not connected.

- After the on-site admin has installed the configlet, the device automatically connects to the management system and the status displays **Update Needed** indicating that the device has connected but the management system has not installed the modeled device configuration yet.

### Installing the Configlet

The on-site admin performs RD in two stages:

- Preparing the security device

- Installing the Configlet

The sections below detail each stage. For detailed, step-by-step instructions on installing the configlet, please see the Rapid Deployment Getting Started Guide.

### Preparing the Device

Before you install the configlet, you must prepare the security device:

1. Connect the device to your network. For details on connecting the device, see the User’s Guide that came with your security device.

2. Connect a standalone computer, such as a laptop, to the device eth1 port.
   - To connect directly to the device, use a cross-over cable.
   - To connect to the device over a hub or switch, use a straight-through cable.

   If your device has auto-sensing ports, you can use any type of Ethernet cable to connect to the device.

3. Change the IP address of the standalone computer to 192.168.1.2 and the default gateway to 192.168.1.1. To change an IP address, see your computer’s operating system documentation.

4. Ensure that the device is using the factory default settings.
   - RD works with the factory default setting of all security devices running ScreenOS 5.x. If the device does not use the factory default settings, you cannot use RD (the WebUI cannot load the configlet).
   - To restore the factory defaults on the firewall device, see the User’s Guide that came with your security device.

5. Ensure that the Status LED on firewall device displays green.
Installing the Configlet

NOTE: During the configlet installation process, you cannot edit the device configuration.

To install the configlet:

1. Save the configlet on the standalone computer that you connected to the security device.

2. In a Web browser, enter the IP address of the trust interface on the security device as 192.168.1.1. The Rapid Deployment Wizard appears.

3. Select Load configlet file and browse to the location of the saved configlet file. Click Next.

   The RD Wizard opens the configlet, authenticates the integrity of the configlet, and decrypts the configlet. If the configlet is valid, the RD Wizard uses the configlet information to prepare the security device for NetScreen-Security Manager management.

4. If prompted, enter the configlet password and click Next. The configlet password is given to you by the NetScreen-Security Manager administrator who sent you the configlet file. Click Next.

5. Confirm or enter the ISP information. The ISP information describes the ISP environment in which the device is deployed. If the NetScreen-Security Manager administrator included ISP information in the configlet, the RD Wizard displays that information. Ensure that all information is correct.

   If the NetScreen-Security Manager administrator did not include ISP information or included only partial information, you must complete the ISP environment for the device:

   - If your firewall device uses DHCP to obtain an IP address from the network, select Using cable modem (Dynamic IP via DHCP).

   - If your firewall device uses a PPPoE connection to the Internet, select Using DSL modem (Dynamic IP via PPPoE). Enter the username and password for your PPPoE account.

   - If your firewall device uses a static IP address, select Using ISP-supplied Settings (Static IP) and enter the IP address, Netmask, and Gateway for the firewall device.

   - If your security device uses a PPPoA connection to the Internet (available on NetScreen-5GT ADSL devices), select PPPoA. Enter the multiplexing mode, VCI/VPI pair, Multiplexing mode, RFC1483 Protocol mode, and the ADSL operating mode for your PPPoA account.

6. Click Next to initiate the connection to NetScreen-Security Manager.
The security device connects to the NetScreen-Security Manager Device Server. During this first connection, the device and the NetScreen-Security Manager Device Server exchange authentication information. After NetScreen-Security Manager authenticates the connection and saves the device public key, it sends a confirmation message to the device, which displays the message in the RD Wizard.

NOTE: For security reasons, after the first successful connection, the security device erases the one-time-password (OTP) from memory.

7. Click close to exit the RD Wizard.

The NetScreen-Security Manager admin can now configure the device using NetScreen-Security Manager.

NOTE: If the configlet installation process fails, you must reset the device to factory defaults. For details, see the User's Guide that came with the security device.

### Updating the Device Configuration

After the on-site admin has installed the configlet and the device has successfully connected to management system, you can install the modeled device configuration on the physical device:

1. Ensure that the device is connected by viewing the device status. Check the device configuration status by holding your mouse cursor over the device in Device Manager (you can also check configuration status in Device Monitor). Ensure that the configuration status for the device displays **Update Needed**, which indicates that the device has connected but the management system has not updated the device configuration yet.

2. Update the device configuration by right-clicking the device and selecting Update Device. The Job Information box appears and displays the job type and status for the update; when the job status displays successful completion, click Close.

After update is complete, the device status displays as **Managed**, indicating that the device has connected and the management system has successfully updated the device configuration.

### Adding Other Device Types

You can also add or import other device types into NetScreen-Security Manager, including:

- Adding Vsys Devices
- Adding an Extranet Device
- Adding a Cluster
- Adding a Vsys Cluster and Vsys Cluster Members
You cannot add multiple vsys, extranet, or cluster devices at one time; you must add each vsys, extranet, and cluster device (and cluster member) individually.

### Adding Vsys Devices

A Virtual System (vsys) is a virtual device that exists within a physical security device. The vsys device functions as a completely separate security device. The physical device, called the root device, can contain multiple vsys devices. The following Juniper Networks security devices can be root devices:

- NetScreen-500
- ISG-1000
- ISG-2000
- NetScreen-5200
- NetScreen-5400

### Placing the Root Device

Before you begin importing or modeling a root device, determine where you want to place the vsys devices:

- To add vsys devices in the global domain and one or more subdomains, add the root device to the global domain.
- To add vsys devices in a single subdomain, add the root device to that subdomain.

An example is shown below:

**Figure 20: Connecting Vsys Devices Across Domains**
Importing Vsycl Devices

Importing vsys devices is a two-stage process where the order is important. You must import the root device first and then import the vsys devices.

The two steps of importing vsys devices are:

- Import the root device—To import the root device, use the Add Device wizard to add the root device to the appropriate domain. For details, see “Importing Devices”.

- Import the vsys devices—To import a vsys device, use the Add vsys wizard to add the vsys device. If you are adding multiple vsys devices to the same domain, you can add them all at once.

To import a vsys device:

1. From the domain menu, select the domain that contains the root device.

2. In Device Manager, click the Add icon and select vsys Device. The Add Device wizard appears.
   - Select the root device for the vsys.
   - Select a color to represent the vsys in the UI.
   - Select Import Existing Virtual System From Physical Device

3. Click Next. Select the domain in which to import the device.

4. Click Next. Select the vsys devices to import:
   - Use SELECT ALL to import all vsys devices from the root device.
   - Use SELECT NONE to clear all checked vsys devices.

5. Click Finish to complete the Add Device wizard. NetScreen-Security Manager automatically imports the select vsys configurations, and the new vsys devices appear in the Device Manager list.

6. To check the device configuration status, mouseover the vsys in Device Manager (you can also check configuration status in Device Monitor):
   - Before the vsys connects, the status displays **Waiting for 1st connect**, indicating that the management system is waiting for the vsys to connect. (This event occurs very quickly and might not display.)
   - After the vsys connects, the status displays **Import Needed**, indicating that the vsys has connected but the management system has not imported the vsys configuration yet.

To view the imported configuration, double-click the vsys in Device Manager.
To check the vsys configuration status, mouseover the vsys device in Device Manager (you can also check configuration status in Device Monitor). The device status displays as **Managed**, indicating that the vsys has connected and the management system has successfully imported the vsys configuration.

**Modeling Vsys Devices**

Modeling vsys devices is a two stage process:

- **Import or Model the root device**—To import or model the root device, use the Add Device wizard to add the root device to the appropriate domain. For details, see “Importing Devices” on page 86 or “Modeling Devices” on page 97.

- **Model the vsys device**—To model a vsys device, use the Add vsys wizard to add the vsys device. You can model a vsys on an imported or modeled root device; however, you cannot update the vsys device configuration until you have first activated the root device. You must model one vsys device at a time.

To model a vsys device:

1. From the domain menu, select the domain that contains the root device.

2. In Device Manager, click the Add icon and select vsys Device. The Add Device wizard appears.

   - Select the root device for the vsys.
   - Select a color to represent the vsys in the UI.
   - Select Model Virtual System Device

3. Click Next to specify the Virtual System information:

   - **NSM vsys Name**. Enter a name for the vsys device. This name identifies the vsys device in the NetScreen-Security Manager UI. The name can contain letters, numbers, spaces, dashes, and underscores.

   - **ScreenOS vsys Name**. Enter a name for the vsys device. This name is stored in the root device. The name can contain letters and numbers and can be no longer than eight characters.

   - **Domain**. Select the domain in which to model the device.

   The wizard automatically complete the vsys ID, device type, and OS version of the root device.

4. Click Next to select the Virtual Router for this device:

   - **Default Vrouter**. Use the default virtual router in the root device.

   - **Shared Vrouter**. Select a one of the virtual routers defined in the root device to be shared with vsys devices.

   - **User Vrouter**. Enter the name of a user-defined virtual router in the root device.
5. Click Finish to complete the Add vsys wizard. The new vsys device appears in the Device Manager list.

6. Ensure that the vsys is connected by viewing the device status. Check the configuration status by holding your mouse cursor over the device in Device Manager (you can also check configuration status in Device Monitor). Ensure that the configuration status for the vsys displays **Update Needed**, which indicates that the device has connected but the management system has not updated the device configuration yet.

7. Update the device configuration by right-clicking the vsys and selecting Update Device. The Job Information box appears and displays the job type and status for the update; when the job status displays successful completion, click Close.

After update is complete, the device status displays as **Managed**, indicating that the device has connected and the management system has successfully updated the device configuration.

After you have modeled the vsys device, create the vsys configuration and update the device. To check the vsys configuration status, mouseover the vsys device in Device Manager (you can also check configuration status in Device Monitor). The device status displays as **Managed**, indicating that the vsys has connected and the management system has successfully updated the vsys configuration.

**Adding L2V Root Systems**

The NetScreen-5000 series security devices running ScreenOS 5.0 L2V also support vsys transparent mode, also known as layer 2 vsys, or L2V vsys. The VLAN Trunk vsys mode and the L2V mode are mutually exclusive; you must enable one or the other on the root system:

- When modeling an L2V root, ensure that the ScreenOS version is set to 5.0L2V and the operating mode is set to Transparent. By default, the root system is modeled as a neutral vsys, enabling you to configure the system in either L2V or VLAN Trunk mode.

- When importing an L2V root:
  - If the device is in transparent mode with L2V enabled, NetScreen-Security Manager imports those settings and creates the device in L2V mode.
  - If the device is transparent mode with L2V disabled, NetScreen-Security Manager creates the device in neutral vsys mode (you can use NetScreen-Security Manager UI to configure the device in VLAN or L2V mode).
  - If the device is transparent mode with VLAN trunk enabled, NetScreen-Security Manager imports those settings and creates the device in VLAN mode. In this mode, you can add vsys devices to the root system, but you cannot import VLAN IDs to those vsys devices.

For details on configuring these vsys modes, see “Converting L2V to VLAN Trunking” on page 362 and “Configuring Layer 2 Vsyst (L2V)” on page 359.
Adding an Extranet Device

An extranet device is a firewall or VPN device that is not a security device. If you use devices from multiple manufacturers, you can add extranet devices to NetScreen-Security Manager to represent your heterogeneous network environment. After you have added the extranet device to the NetScreen-Security Manager UI, you can use the device in groups, Security Policies, and VPNs.

To add a new extranet device in Device Manager, click the add icon and select Extranet device. The Extranet Device dialog box appears. Enter the extranet device information:

- **Name**—Enter the name of the extranet device. The name can contain letters, numbers, spaces, dashes, and underscores.
- **Color**—Select the color that represents the extranet device in the NetScreen-Security Manager UI.
- **IP Address**—Enter the IP Address of the extranet device

Click OK to add the extranet device to NetScreen-Security Manager.

Adding a Cluster

A cluster is a two security devices joined together in a high availability configuration to ensure continued network uptime. The two device configurations are synced, meaning both devices share the same configuration settings, enabling either device to handle traffic for the other if one device fails.

Adding a cluster is a two stage process:

1. Add the cluster device object.
2. Add the members of the cluster to the cluster device object. *(When importing cluster members, ensure that their device configurations are in sync.)*

Adding a Cluster Device Object

In Device Manager, click the Add icon and select Cluster. Enter the cluster information:

- **Cluster Name**—Enter a name for the cluster.
- **Color**—Select a color to represent the cluster.
- **Physical Choice**—Select the security device platform for both cluster members.
- **OS Version**—Select the ScreenOS version for both cluster members.
- **Transparent Mode**—Enable transparent mode, if desired.

The cluster device object appears in the device tree.
Adding Members to the Cluster

Next, add the members of the cluster to the cluster device object. In Device Manager, right-click the Cluster device and select New > Cluster Member. The Add Device wizard appears; follow the instructions in the wizard to import or add a new cluster member.

- When importing cluster members, first ensure that their configurations are in sync. Next, use the Add Device Wizard to automatically import the device configurations from each physical cluster device member.

- When modeling a cluster member, ensure that both cluster members have been added to the cluster device object before configuring the cluster.

By default, the cluster propagates settings made in one device member to the other device member. However, the following settings are not propagated and must be configured on each device in the cluster: VSD group, VSD priority, authentication and encryption passwords, manage IP addresses, and IP tracking settings. All other commands are propagated among devices within the cluster.

For details on creating and configuring a cluster, see “Configuring NSRP Clusters” on page 376. For example, to create a cluster that includes an existing device (with an existing configuration and Security Policy) and a new device (with no configuration or Security Policy), you should:

1. Create the cluster.

2. Add the existing device by importing. The Add Device Wizard automatically imports the device configuration.

3. Add the new device by modeling, then activating the device.

Adding a Vsys Cluster and Vsys Cluster Members

A vsys cluster is a vsys device that has a cluster as its root device. Adding a vsys cluster is a three stage process:

1. Add a cluster device object. For details on adding a cluster, see “Adding a Cluster” on page 115. (You add members later.)

2. Add a vsys device that uses the cluster device as root. For details on adding a vsys device, see “Adding Vsys Devices” on page 111.

3. Add the two cluster members to cluster device, using the instructions in the wizard to import or add a new cluster member. After adding the two cluster members, UI displays each cluster member as a member of the cluster device.

The UI also creates a vsys cluster member for each vsys device that uses the cluster as its root device. The vsys cluster member contains local information; the cluster member contains the global information. Although a cluster can have only two members, a root vsys device can support more than two vsys devices.

EXAMPLE: ADDING A VSYS CLUSTER
In this example, you add a vsys cluster with two members and two vsys.
1. **Add the cluster device:**
   a. In the main navigation tree, select Device Manager > Security Devices. Click the Add icon and select Cluster. The new cluster dialog box appears. Configure as detailed below:
      - For Name, enter Paris Cluster.
      - For Physical Choice, select ns5400.
      - For OS Version, select 5.1.
   b. Click OK to save the new cluster object.

2. **Add the first Vsys device:**
   a. Click the Add icon and select Vsys Device. The new Vsys device dialog box appears.
   b. Configure the root as the Paris Cluster device, select a color, and choose Model Virtual System/Virtual System Cluster Device. Click Next to continue.
   c. Configure the NetScreen-Security Manager and ScreenOS name as Paris V1, then select global as the domain. Click Next to continue.
   d. Configure the vrouter for the vsys as the Default Vrouter, then click Next to continue.
   e. Click Finish to add the new vsys cluster device.

3. **Add the second vsys cluster device:**
   a. Click the Add icon and select Vsys Device. The new Vsys device dialog box appears.
   b. Configure the root as the Paris Cluster device, select a color, then select Model Virtual System/Virtual System Cluster Device. Click Next to continue.
   c. Configure the NetScreen-Security Manager and ScreenOS name as Paris V2, then select global as the domain. Click Next to continue.
   d. Configure the vrouter for the vsys as the Default Vrouter, then click Next to continue.
   e. Click Finish to add the new vsys cluster device.

   The Paris Cluster and Paris V1 devices now appear in the security device tree.

4. **Add cluster members:**
   a. In the main display area, right-click Paris Cluster and select New > Cluster Member. The New Cluster Member dialog box appears.
   b. Configure the cluster members OfficeA and OfficeB as shown below:
As you add each cluster member, NetScreen-Security Manager automatically creates both the cluster member and the vsys cluster member. In the security device tree, the Paris Cluster (and cluster members) and Paris vsys cluster (and cluster member) appear as shown below:
Adding Many Devices

If your network includes a large number of security devices, adding each device individually can take unwanted time and effort. To help you import or model your existing devices into NetScreen-Security Manager, you can now add multiple devices in a single workflow using the Add Many Device wizard.

With the wizard, you can add up to 4000 devices at a time to a single domain (you cannot add multiple devices to different domains at one time). Additionally, you can create configlets for and activate newly deployed security devices that are running ScreenOS 5.x; however, you cannot configure Rapid Deployment when adding many security devices that are systems (NetScreen-500, NetScreen-5000, ISG 1000, ISG 2000).

NOTE: You cannot add Cluster or Cluster Members using the Add Many Device wizard.

Adding many devices is a three step process:

1. Create the CSV file. This file defines all the required and optional values for each device.

2. Using the Add Many Devices wizard, select the CSV file to import or model the devices. The wizard first validates the CSV file and notifies you of any errors, then adds the devices for which all defined values are valid.

   - When importing devices with static IP addresses, the device configuration is automatically imported during the Add Many Devices workflow.
When importing devices with dynamic IP addresses, you must manually import the device configuration after the Add Many Device workflow is complete.

When modeling ScreenOS 5.x devices for Rapid Deployment, you can also create configlets during the Add Many Devices workflow, or select to skip configlet creation.

The time it takes for NetScreen-Security Manager activate and import devices depends on the number of devices and the management system configuration.

3. Verify the device configuration.

The following sections detail each step.

Creating the CSV File

Within a .csv file, you define the device configuration values for each device you want to add. The required and optional values depend on how the device is deployed on your network: static IP addresses, dynamic IP addresses, or undeployed devices.

NOTE: When adding security devices running ScreenOS 4.x that use NACN, you must specify the NACN interface (the interface that NetScreen-Security Manager uses to manage NACN).

You must create a separate CSV file for the following devices:

- Devices with known IP addresses—In this CSV file, you define the device parameters required to add and import the device configurations from ScreenOS 4.0.x and 5.x devices.

- Devices with unknown IP addresses—In this CSV file, you define the device parameters required to add ScreenOS 4.0.x and 5.x devices to the NetScreen-Security Manager system.

- Undeployed devices—In this CSV file, you define the device parameters required to add and model the devices in the NetScreen-Security Manager system.

NOTE: You can model many devices, but you cannot activate many devices except when using the Rapid Deployment process.

Juniper Networks provides csv templates in Microsoft Excel format for each type of csv file; templates are located on the Juniper Networks support Web site.

For each csv file, the header row defines the required and optional parameters; each subsequent row defines a single device’s values for those parameters. Columns are separated by commas.

Devices with Static IP Addresses

For devices with static IP addresses, create a .csv file with the following parameters:

-
Table 9: CSV File Information for Devices with Static IP Addresses

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Type</th>
<th>Required</th>
<th>Acceptable Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>String</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>Color</td>
<td>String</td>
<td>yes</td>
<td>black, gray, blue, red, green, yellow, cyan, magenta, orange, pink</td>
</tr>
<tr>
<td>Device IP Address</td>
<td>String</td>
<td>yes</td>
<td>192.168.1.1, 10.1.1.10, 3.3.3.3</td>
</tr>
<tr>
<td>Device Admin Name</td>
<td>String</td>
<td>yes</td>
<td>&lt;admin&gt;</td>
</tr>
<tr>
<td>Device Admin Password</td>
<td>String</td>
<td>yes</td>
<td>&lt;password&gt;</td>
</tr>
<tr>
<td>Connection Protocol</td>
<td>String</td>
<td>yes</td>
<td>telnet, ssh_v1, ssh_v2</td>
</tr>
<tr>
<td>Device Admin Port</td>
<td>Integer</td>
<td>no</td>
<td>23, 22, 4444, 7777</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>If null, uses 23 for telnet and 22 for SSH</td>
</tr>
<tr>
<td>SSH Fingerprint</td>
<td>String</td>
<td>yes (when connection SSH)</td>
<td></td>
</tr>
<tr>
<td>Global Pro Logging</td>
<td>String</td>
<td>yes</td>
<td>on, off</td>
</tr>
<tr>
<td>NACN</td>
<td>String</td>
<td>yes</td>
<td>on, off</td>
</tr>
<tr>
<td>NACN Interface Monitored</td>
<td>String</td>
<td>yes (when NACN is enabled)</td>
<td></td>
</tr>
<tr>
<td>NACN Password</td>
<td>String</td>
<td>yes (when NACN is enabled)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>must be a valid device interface</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>must be a minimum of 9 characters</td>
</tr>
</tbody>
</table>

**EXAMPLE: USING AN EXCEL FILE TO ADD MULTIPLE STATIC IP DEVICES**
To view the template for adding many device with static IPs:
1. Download the Microsoft Excel file Add_Many_Devices_Reachable.xls from the Juniper Networks support Web site. The header row at the top defines the settings.
2. Using one row for each device you want to add, enter the required values for the device. You can also provide optional values, if desired.
3. Save the file to a location on your local drive.

**EXAMPLE: USING A TEXT FILE TO ADD MULTIPLE STATIC IP DEVICES**
To add two security devices that use static IP addresses, create a text file with the following text:

```plaintext
Chicago,green,10.100.31.78,netscreen,netscreen,ssh_v2,,any,on,off,,,Memphis,orange,10.100.20.236,netscreen,netscreen,ssh_v2,,any,on,off,untrust,password,Columbus,red,10.100.20.200,netscreen,netscreen,telnet,,any,off,off,,,Cincinnati,blue,10.100.20.237,netscreen,netscreen,ssh_v2,,any,on,untrust,pw-nacn,
```

After you have created the file, save it as a .csv file.
Device with Dynamic IP Addresses

For devices with dynamic IP addresses, create a .csv file with the following parameters:

Table 10: CSV File Information for Devices with Dynamic IP Addresses

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Type</th>
<th>Required</th>
<th>Acceptable Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>String</td>
<td>yes</td>
<td>dev1, Chicago, NS-208</td>
</tr>
<tr>
<td>Color</td>
<td>String</td>
<td>yes</td>
<td>black, gray, blue, red, green, yellow, cyan, magenta, orange, pink</td>
</tr>
<tr>
<td>Device Platform</td>
<td>String</td>
<td>yes</td>
<td>nsSGT-Combined, nsSGT-Dual-Untrust, nsSGT-Trust-Untrust, nsSGT-Trust-Untrust-DMZ, nsSGTadsl-Home-Work, nsSGTadsl-Trust-Untrust, nsSGTadsl-Trust-Untrust-DMZ, ns5XP, ns5XT, ns5XT-Combined, ns5XT-Dual-Untrust, ns5XT-Trust-Untrust, ns25, ns50, ns100, ns204, ns208, ns500, ns5200, ns5400, nsHSC-Home-Work, nsHSC-Trust-Untrust, nsISG1000, nsISG2000, nsISG1000, nsISG1000</td>
</tr>
<tr>
<td>ScreenOS Version</td>
<td>String</td>
<td>yes</td>
<td>5.x, 4.0.x</td>
</tr>
<tr>
<td>Transparent Mode</td>
<td>String</td>
<td>yes</td>
<td>on, off</td>
</tr>
<tr>
<td>License Key Model</td>
<td>String</td>
<td>yes</td>
<td>range of values defined in dcf file</td>
</tr>
<tr>
<td>First Conn OTP</td>
<td>String</td>
<td>yes (when using ScreenOS 5.x)</td>
<td></td>
</tr>
<tr>
<td>Device Serial Number</td>
<td>String</td>
<td>yes (when using ScreenOS 4.0.x)</td>
<td></td>
</tr>
<tr>
<td>NACN Interface</td>
<td>String</td>
<td>yes (when using ScreenOS 4.0.x)</td>
<td>must be a valid device interface</td>
</tr>
<tr>
<td>Global Pro Logging</td>
<td>String</td>
<td>yes</td>
<td>on, off</td>
</tr>
<tr>
<td>Device Admin Name</td>
<td>String</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>Device Admin Password</td>
<td>String</td>
<td>yes</td>
<td>must be a minimum of 9 characters</td>
</tr>
<tr>
<td>Telnet Port</td>
<td>Integer</td>
<td>no</td>
<td>if null, defaults to 23</td>
</tr>
<tr>
<td>SSH Port</td>
<td>Integer</td>
<td>no</td>
<td>if null, defaults to 22</td>
</tr>
</tbody>
</table>

EXAMPLE: USING AN EXCEL FILE TO ADD MULTIPLE DYNAMIC IP DEVICES

To view the template for adding many device with dynamic IPs:

1. Download the Microsoft Excel file Add_Many_Devices_Unreachable.xls from the Juniper Networks support Web site. The header row at the top defines the settings.

2. Using one row for each device you want to add, enter the required values for the device. You can also provide optional values, if desired.
3. Save the file to a location on your local drive.

EXAMPLE: USING A TEXT FILE TO ADD MULTIPLE DYNAMIC IP DEVICES
To add two security devices that use dynamic IP addresses, create a text file with the following text:

```
dev03,red,ns204,5.0,off,advanced,netscreen123,43042002000071,,off,netscreen-super,netscreen,,
dev04,green,ns500,5.0,off,advanced,netscreen123,10062002000039,,off,super-netscreen,netscreen,,
```

After you have created the file, save it as a .csv file.

Undeployed Devices
For undeployed devices (ScreenOS 5.x only), create a .csv file with the following parameters:

Table 11: CSV File Information for Undeployed Devices

<table>
<thead>
<tr>
<th>Field name</th>
<th>Type</th>
<th>Required</th>
<th>Acceptable Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>String</td>
<td>yes</td>
<td>valid character</td>
</tr>
<tr>
<td>Color</td>
<td>String</td>
<td>yes</td>
<td>black, gray, blue, red, green, yellow, cyan, magenta, orange, pink</td>
</tr>
<tr>
<td>Platform</td>
<td>String</td>
<td>yes</td>
<td>must be a device platform that supports ScreenOS 5.x and configlets (cannot be a ns5GADSL device)</td>
</tr>
<tr>
<td>ScreenOS Version</td>
<td>String</td>
<td>yes</td>
<td>must be a ScreenOS 5.x device platform</td>
</tr>
<tr>
<td>Transparent Mode</td>
<td>String</td>
<td>yes</td>
<td>on, off</td>
</tr>
<tr>
<td>License Key Model</td>
<td>String</td>
<td>yes</td>
<td>range of values defined in dcf file</td>
</tr>
<tr>
<td>First Conn OTP</td>
<td>String</td>
<td>yes</td>
<td>must be a minimum of 9 characters</td>
</tr>
<tr>
<td>Connection Type</td>
<td>String</td>
<td>yes</td>
<td>static, pppoe, dhcp, prompt</td>
</tr>
<tr>
<td>Device IP Address</td>
<td>String</td>
<td>yes (when connection type is static)</td>
<td>8, 24, 32, Any valid netmask in CIDR format</td>
</tr>
<tr>
<td>Device Netmask</td>
<td>String</td>
<td>yes (when connection type is static)</td>
<td>8, 24, 32, Any valid netmask in CIDR format</td>
</tr>
<tr>
<td>Device Gateway</td>
<td>String</td>
<td>yes (when connection type is static)</td>
<td>8, 24, 32, Any valid netmask in CIDR format</td>
</tr>
<tr>
<td>PPPoE User Name</td>
<td>String</td>
<td>yes (when connection type is PPPoE)</td>
<td>must be a minimum of 9 characters</td>
</tr>
<tr>
<td>PPPoE User Password</td>
<td>String</td>
<td>yes (when connection type is PPPoE)</td>
<td>must be a minimum of 9 characters</td>
</tr>
<tr>
<td>Configlet Password</td>
<td>String</td>
<td>no</td>
<td>default to a random string between 9 and 256 characters</td>
</tr>
<tr>
<td>Device Admin Name</td>
<td>String</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>Device Admin Password</td>
<td>String</td>
<td>yes</td>
<td>must be a minimum of 9 characters</td>
</tr>
<tr>
<td>Telnet Port</td>
<td>Integer</td>
<td>no</td>
<td>default to 23</td>
</tr>
</tbody>
</table>
EXAMPLE: USING AN EXCEL FILE TO ADD MULTIPLE MODELED DEVICES

To view the template for adding many modeled devices:

1. Download the Microsoft Excel file Add_Many_Devices_Model.xls from the Juniper Networks support Web site. The header row at the top defines the settings.

2. Using one row for each device you want to add, enter the required values for the device. You can also provide optional values, if desired.

3. Save the file to a location on your local drive.

EXAMPLE: USING A TEXT FILE TO ADD MULTIPLE MODELED DEVICES

To add and model three security devices, create a text file with the following text:

```plaintext
dev13,orange,ns5XP,5.0,off,advanced,netscreen123,static,10.10.30.5,32,10.10.30.1,,,123456abc,netscreen,netscreen123,,
dev14,green,ns50,5.0,off,advanced,netscreen123,pppoe,,,,root,netscreen,,1netscreen,netscreen1,,
dev15,red,ns204,5.0,off,advanced,netscreen123,dhcp,,,,,,,2netscreen,netscreen2,,
```

After you have created the file, save it as a .csv file.

Validating the CSV file

When you add the device, NetScreen-Security Manager validates the configuration information in the .csv file and creates a Validation Report. The report lists any incorrect or duplicate configurations, and indicates the exact line that contains invalid data.

NOTE: The Validation Report displays only the first error in the line. If the line contains additional errors, those errors do not appear in the Validation Report.

Select Cancel to quit the Add Many Devices process, or select Add Valid Devices to begin adding the devices for which you have provided valid device configurations. If the Validation Report listed incorrect configurations, you can still select Add Valid Devices; however, only the devices with correct configurations are added. If the .csv file contains duplicate configurations, NetScreen-Security Manager ignores the duplicates.

After you have added device, you cannot rollback or undo your changes. To edit or delete a device, select the device in the UI and make the necessary changes.

Importing Many Devices

The import process differs slightly between devices that use static IP addresses and devices that use dynamic IP addresses:
For devices with static IP addresses, the Add Many Devices wizard automatically imports the device configurations.

For devices with dynamic IP addresses, you must manually import the device configurations.

In some cases, you might also need to configure NACN, or other features on the physical device to enable the device to connect to NetScreen-Security Manager.

After you have added the devices, you should take a moment to verify that the device configuration import matches your expectations. For details, see “Verifying Imported Device Configurations” on page 94.

Adding Many Devices with Static IP Addresses

For devices with static IP addresses:

1. From the domain menu, select the domain in which to import the device.
2. In Device Manager, click the Add icon and select Many Devices. The Add Device wizard appears.
   - Select Device is Reachable (default).
   - Specify the location of the CSV file.
3. Click Next. The Add Device wizard validates the CSV file and provides a Validation Report:
   - Select Cancel to quit the Add Many Devices process.
   - Select Add Valid Devices to begin adding the devices for which you have provided valid device configurations.

The Add Device wizard adds the valid devices and automatically imports their configurations.

Adding Many Devices with Dynamic IP Addresses

For devices with dynamic IP addresses:

1. From the domain menu, select the domain in which to import the device.
2. In Device Manager, click the Add icon and select Many Devices. The Add Device wizard appears.
   - Select Device is Not Reachable.
   - Specify the location of the CSV file.
   - Specify the output directory for the .cli file. For each valid ScreenOS device configuration that uses a dynamic IP address, NetScreen-Security Manager creates a .cli output file. During the add process, you can specify the directory (Cli Server Output Subdir) that should be used to save the .cli file. By default, the .cli file is saved to the following GUI Server directory:
Before the device can be managed by NetScreen-Security Manager, you must enter the CLI commands in the .cli file on the physical security device.

3. Click Next. The Add Device wizard validates the CSV file and provides a Validation Report:

- Select Cancel to quit the Add Many Devices process.
- Select Add Valid Devices to begin adding the devices for which you have provided valid device configurations.

4. The Add Device wizard adds the valid devices and automatically imports their configurations.

**Modeling Many Devices**

For undeployed devices, you can create their device configurations in NetScreen-Security Manager in a single workflow. After you have created modeled configurations for each device, you must activate all devices individually.

---

NOTE: The devices must be running ScreenOS 5.x.

To model many devices:

1. From the domain menu, select the domain in which to import the device.

2. In Device Manager, click the Add icon select Many Devices. The Add Device wizard appears.

   - Select Model Device.
   - Specify the location of the CSV file.

3. Click Next. The Add Device wizard validates the CSV file and provides a Validation Report:

   - Select Cancel to quit the Add Many Devices process.
   - Select Add Valid Devices to begin adding the devices for which you have provided valid device configurations.

   The Add Device wizard adds the valid devices to the NetScreen-Security Manager UI.

4. Model the device configuration as desired.

After you have added the device and created modeled device configurations for your undeployed device, you are ready to activate the device and prompt it to connect to the management system. After that device has made contact with NetScreen-Security Manager, you can install the modeled configuration you created on the physical device. For details on activating a device, see “Activating a Device” on page 98.
Using Rapid Deployment

You can model, generate configlets, and activate many ScreenOS 5.x devices at one time. Alternatively, you can choose to model multiple devices initially, then generate configlets and activate them at a later time. The devices must be running ScreenOS 5.x and support configlets; NetScreen systems (NetScreen-500, 5000 series, ISG 1000, and ISG 2000) do not support configlets.

Modeling and Activating Many Devices (with Configlets)

To model, create configlets, and activate at the same time:

1. From the domain menu, select the domain in which to import the device.

2. In Device Manager, click the Add icon and select Many Devices. The Add Device wizard appears.
   - Select Model Device.
   - Specify the location of the CSV file.
   - Select Activate and Create Configlets now (ns208 and below).
   - Specify the output directory for the .cfg file. For each modeled ScreenOS 5.x device configuration, NetScreen-Security Manager creates a .cfg output file. During the configlet creation process, you can specify the directory (Configlet Server Output Subdir) that should be used to save the .cfg file. By default, the .cfg file is saved to the following GUI Server directory:

     /usr/netscreen/GuiSvr/var/ManyDevicesOutput/<inputFile_YYYYMMDDHHMM>

3. Click Next. The Add Device wizard validates the CSV file and provides a Validation Report:
   - Select Cancel to quit the Add Many Devices process.
   - Select Add Valid Devices to begin adding the devices for which you have provided valid device configurations.

   The Add Device wizard adds the valid devices to the NetScreen-Security Manager UI.

4. Send the .cfg file to the on-site administrator for the corresponding device. After the on-site administrator installs the configlet on the physical security device, the device automatically contacts the NetScreen-Security Manager Device Server, which establishes an always-on management connection. For instructions for the on-site administrator, see “Installing the Configlet” on page 108, or refer to the Rapid Deployment Getting Started Guide.

5. Model the device configurations as desired.

6. Install the modeled configuration. After the on-site administrators have installed the configlets and the devices have successfully connected to management system, you can install the modeled device configurations on the physical devices:
a. Ensure that the device is connected by viewing the device status. Check the device configuration status by holding your mouse cursor over the device in Device Manager (you can also check configuration status in Device Monitor). Ensure that the configuration status for the device displays **Update Needed**, which indicates that the device has connected but the management system has not updated the device configuration yet.

b. Update the device configuration by right-clicking the device and selecting Update Device. The Job Information box appears and displays the job type and status for the update; when the job status displays successful completion, click Close.

After update is complete, the device status displays as **Managed**, indicating that the device has connected and the management system has successfully updated the device configuration.

For more details on the Rapid Deployment, see “Using Rapid Deployment” on page 104.

Activating Many Devices (with Configlets)

Before activating devices and creating a configlet, you must configure a modeled configuration for the device in the NetScreen-Security Manager UI.

To create configlets and activate many devices:

1. In Device Manager, click the Add icon and select Activate Many Devices. The Activate Device wizard appears.

2. Select the devices to activate.

3. Specify the output directory for the .cfg file. For each modeled ScreenOS 5.x device configuration, NetScreen-Security Manager creates a .cfg output file. During the configlet creation process, you can specify the directory (Configlet Server Output Subdir) that should be used to save the .cfg file. By default, the .cfg file is saved to the following GUI Server directory:

   `/usr/netscreen/GuiSvr/var/ManyDevicesOutput/<inputFile_YYYYMMDDHHMM>/`

4. Send the .cfg file to the on-site administrator for the corresponding device. After the on-site administrator installs the configlet on the physical security device, the device automatically contacts the NetScreen-Security Manager Device Server, which establishes an always-on management connection. For instructions for the on-site administrator, see “Installing the Configlet” on page 108, or refer to the Rapid Deployment Getting Started Guide.

5. Click OK. A Job Manager window appears to display the progress of the activation. When completed, click Close.

6. Update the physical device with the modeled configuration.

**NOTE:** For security reasons, you cannot edit a configlet file directly. To make changes to the information in any configlet file, run the Activate Many Device wizard to re-generate the configlets.
Chapter 5
Configuring Devices

The Device Manager module in Juniper Networks NetScreen-Security Manager enables you to configure the managed Juniper Networks security devices in your network. You can edit configurations after you add or import a managed device, or create configurations when you model a device. For details about adding, importing, or modeling a device, see Chapter 4, “Adding Devices”.

This chapter details the device configuration parameters, and provides configuration examples when possible. For step-by-step instructions on configuring specific device settings, see the NetScreen-Security Manager Online Help. This chapter also details two important tools that you can use to simplify configuring multiple security devices: templates and device groups.

The following sections are in this chapter:

- About Device Configuration
- Using Templates
- Using Device Groups
- Configuring Device Information
- Configuring Network Overview
- Configuring Wireless Settings
- Configuring the Network Module
- Configuring Virtual Routers
- Configuring Dynamic Routing
- Configuring Multicast Routing
- Configuring Zones
- Configuring Interfaces
- Configuring DIP Groups
- Configuring PPPoE
- Configuring PPPoA
- Configuring NACN
- Configuring Modem Connection
- Configuring DNS
- Configuring Advanced Network Settings
- Configuring Device Administration
- Configuring Authentication
- Configuring Reporting
- Configuring Security
- Configuring Advanced Device Settings
- Configuring L2TP and XAuth Local Users
- Configuring vsys
- Configuring Certificates
- Configuring NSRP Clusters

After you edit or create a configuration for a device, you must update the configuration on the managed device for your changes to take effect. For details on updating devices, see Chapter 6, “Updating Devices”.
Use Security Policies to configure firewall and VPN rules that control traffic on your network, as described in Chapter 9, “Configuring Security Policies”. Use the VPN Manager to configure VPNs, as described in Chapter 10 “Configuring VPNs”.

About Device Configuration

The device configuration contains the configuration settings for a managed device, such as interface, routing, and authentication settings. You can edit configurations after you add or import a managed device, or create configurations when you model a device. When you are satisfied with your changes, you can then update the managed device with the modeled device configuration to make your changes effective.

NOTE: When you open a device for viewing or editing, the NetScreen-Security Manager UI loads the entire device configuration into memory to enhance UI performance while configuring the device. When you close a device to which you made changes, the UI unloads some of the device configuration from the client memory. Although this memory optimization occurs quickly, you might see the following message appear: “Optimizing client memory usage for device”.

NetScreen-Security Manager does not support all device configuration settings; you may need to make some changes (described below) to the device locally, using the Juniper Networks ScreenOS WebUI or CLI. Additionally, some changes can affect the management connection between the NetScreen-Security Manager Device Server and the managed device.

About Configuring Security Devices

A security device provides perimeter and boundary protection using data encryption, authentication, access control, and some attack detection and prevention. Firewalls and virtual private networks (VPNs) are designed for high speed operation at the network layer.

While firewalls provide protection, there are attacks contained within the allowed traffic that firewalls are not designed to detect.

About Configuring IDP-Capable Devices

Juniper Networks Intrusion Detection and Prevention (IDP) technology can both detect and then stop attacks when deployed inline to your network. Unlike IDS, IDP uses multiple methods to detect attacks against your network and prevent attackers from gaining access and doing damage. IDP can drop malicious packets or connections before the attacks can enter your network. IDP is designed to reduce false positives and ensure that only actual malicious traffic is detected and stopped. You can also deploy IDP as a passive sniffer, similar to a traditional IDS, but with greater accuracy and manageability.
NetScreen-Security Manager is the sole means for configuring and managing IDP on the ISG 2000 and ISG 1000 devices. The ISG 2000 and ISG 1000 security module, an optional component installed in the device, provides IDP functionality. If you purchased a ISG 2000 or ISG 1000 device that does not have IDP capability, you can upgrade the device to be an IDP-capable system by replacing the memory chip in the CPU, installing up to three security modules, and installing the Advanced and IDP license keys for IDP.

You can use the ISG 2000 or ISG 1000 device with IDP capability as a fully-integrated FW/VPN/IDP security system that not only screens traffic between the Internet and your private network, but also provides application-level security. You can also use the ISG 2000 or ISG 1000 device as a standalone IDP system to protect critical segments of your private network.

NOTE: Juniper Networks offers “standalone” NetScreen-IDP appliances that provide IDP functionality without integrated FW/VPN capabilities. You cannot use the NetScreen-Security Manager system to manage these appliances. NetScreen-Security Manager supports IDP only on the ISG 2000 and ISG 1000 devices.

About Configuring Devices Running ScreenOS 5.0 FIPS

The following features are disabled on security devices running the Federal Information Processing Standards (FIPS) certified release of ScreenOS (ScreenOS 5.0FIPS):

- SNMP management
- MD5 algorithm use
- Group 5 Phase 2 IKE proposals

For more information on FIPS-enabled security devices, refer to the ScreenOS 5.0FIPS Reference Note.

NOTE: To configure and manage security devices running ScreenOS 5.0FIPS using NetScreen-Security Manager, you must first configure a VPN tunnel between the device and the NetScreen-Security Manager GUI Server. After establishing this tunnel, you can not reconfigure tunnel parameters in NetScreen-Security Manager.

About Configuring Devices Running Future Releases of ScreenOS

You can use NetScreen-Security Manager to configure security devices running future releases of ScreenOS in one of three levels of support:

- Forward Support (Basic)—when a new version of ScreenOS is available, you can download a schema patch which includes changes to the DCF and schema files, as well as the firmware tables, enabling you to manage devices using a previously known version of ScreenOS.
Forward Support (Blended)—when a new version of ScreenOS is available, you can download a schema patch, enabling you to manage devices using the new ScreenOS version. You can not, however, manage the new features in ScreenOS with this level of support.

Full Support—when a new version of ScreenOS is available, you can download a schema patch, enabling you to manage devices using the new ScreenOS version. In addition, you can also manage all the new features in that version of ScreenOS.

The Support Level is indicated in the Information screen for the device in the Device Manager.

Unsupported Changes

Some device configurations can be performed only by the device administrator using the CLI or WebUI. A NetScreen-Security Manager administrator cannot perform the following device configurations in the Device Manager:

- Configuring functions that are only applicable for the device administrator, such as setting initial IKE contact, audible alarms, MAC addresses, or console operations.
- Configuring functions that require device administrator intervention, such as Secure Command Shell (SCS) and Secure Shell (SSH) client operation.
- Executing debugging commands.

Changes that Affect the Management Connection

Some configuration changes to a managed device can affect the NetScreen-Security Manager connection to the device when you update the device, such as:

- Changing the connection method (Telnet or SSH) used between the NetScreen-Security Manager Device Server and the managed device.
- Disabling the ability of the managed device to communicate with the NetScreen-Security Manager Device Server.
- Changing the IP address of the NetScreen-Security Manager Device Server on the managed device.
- Changing the interface on the managed device that is permitted to receive NetScreen-Security Manager management traffic.
- Changing the VPN that handles traffic between the managed device and the NetScreen-Security Manager Device Server.
- Modifying router information on the managed device.
- Changing Security Policy rules on the managed device that cause NetScreen-Security Manager traffic to be dropped.
If you need to make any of the above changes to the managed device, use the WebUI or CLI to make the changes locally, then re-import the device configuration into the NetScreen-Security Manager UI.

---

**NOTE:** When you re-import a device configuration, you must also re-assign a Security Policy to the re-imported device.

---

### Determining Device Configuration Status

You can view the connection and configuration status for each managed device in Device Manager.

NetScreen-Security Manager automatically updates the device status and displays the state of each device in the UI. To view device status, simply place your mouse cursor over the device name. A tooltip appears stating the device name, device type and ScreenOS version, IP address, domain, and the connection and configuration states.

---

**NOTE:** Detailed configuration status is not supported for devices running ScreenOS 4.0.x or 5.0.x.

---

For details on viewing device status, see “Verifying Device Status in Device Monitor” on page 400.

---

### Using Templates

Use templates to define a common device configuration and then reuse that configuration information across multiple devices. In a template, you can define only those configuration parameters that you want to set; you do not need to specify a complete device configuration. Templates provide two benefits:

- You can configure parameter values for a device by referring to one or more templates when configuring the device.
- When you change a parameter value in a template and save the template, the value also changes for all device configurations that refer to that template. See “Modifying Template Values” on page 143.

When you apply a template to a device, NetScreen-Security Manager applies the template settings to the device. For example, you can create a template that specifies the IP address of the NTP server to which all managed security devices synchronize their clocks. You can apply this template to the configuration of each device in your domain so that all devices use the same NTP server. You can apply the same template to different types of security devices, from NetScreen-5XT appliances to NetScreen-5200 systems.
A template can refer to other templates, enabling you to combine multiple templates into a single template. When you make changes to any of the referenced templates, those changes are propagated through the combined template. For more information about the options you can configure, see the later sections in this chapter, starting with “Configuring Device Information” on page 149. For step-by-step instructions on creating and applying templates, see the NetScreen-Security Manager Online Help topic, “Adding Device Templates” and “Applying Templates”.

Changing Values Set By Templates

You can manually override any value set by a template in the individual device configuration. To determine if the value is set by a template or is device-specific, press the SHIFT key and move the mouse cursor over the field name:

- If the value is set by a template, the message “From template: template-name” appears, as shown below:

  Figure 23: View Template Override Message

- If the value is set by the individual device (a device-specific value), the “From object” appears.

For any value in the device configuration that was set by a template, select the value and use SHIFT-RIGHTCLICK to automatically revert the device-specific value to the template-defined value (this also reverts non-template values back to the default value). An example is shown below:
A device-specific configuration value always overrides a template value.

In addition, if a device has a policy set to none or Please select, templates will not override these values, since they are set by a user. You can remove these values with the procedure described above.

**Template Limitations**

When configuring and using templates in NetScreen-Security Manager, be aware of the following limitations.

**Maximum of 63 Templates**

You can apply a maximum of 63 templates to a single device. However, configuring certain features reduces the maximum number of templates you can apply to a device:

- Cluster or vsys member—Configuring a device as a vsys device or as a member of a cluster reduces the maximum number of templates by one.

- VPNs—Each VPN that the device belongs to also reduces the maximum number of templates by one. This includes VPNs configured in VPN Manager and VPNs configured at the device-level.

- Referenced templates—Each referenced template (a template referred to by another template) reduces the maximum number of templates by one. For example, a device that uses template A, which in turn refers to templates B and C, calculates three templates applied to the device.

**Device Groups**

You cannot apply a template to a device group. To use the same template for multiple devices, you must apply the template to each device individually.
Default Values
When creating a template, default values do not appear, as many default values depend on the Juniper Networks ScreenOS version and device platform.

Device Entities
Templates do not automatically include any of the entities that are predefined on devices, such as zones, interfaces, or virtual routers. To create a template that refers to a specific predefined entity, you must create the entity in the template.

For example, to create a template that refers to the ethernet1 interface:

1. In the template navigation tree, select Network > Interface.
2. Click the Add icon and select Predefined Interface. The Physical Interface dialog box appears.
3. For Name, enter ethernet1.

NOTE: When creating or editing predefined interfaces in a template, you must use full names for the interface (such as trust, untrust, ethernet1, ethernet1/2, etc...). Do not use names in short form (i.e., eth2/x instead of ethernet2/x).

When adding an entity in a template, ensure that the menu option you select is appropriate for the predefined entity. Choose the menu option that includes the name of the predefined entity you are creating.

For example, to create a template that refers to the mgt zone:

1. In the template navigation tree, select Network > Interface.
2. Click the Add icon and select Predefined Functional Zone > mgt/vlan. The Zone dialog box appears.
3. Enter mgt.

Key List Parameters
Key list parameters uniquely identify a configuration object in a list of similar objects and are read-only. You cannot edit key list parameters that are derived from a template. For example, a zone name uniquely identifies a zone in a list of zones that can be configured on a device. If you create a zone in a template and apply the template to a device, you cannot change the zone name in the device configuration. You must first delete the template-derived zone, then create a new zone.

A configuration object can contain multiple key list parameters. For example, in the routing table, multiple parameters (including IP address/netmask, interface, next-hop, vsys, and so on) uniquely identify a particular route entry.

EXAMPLE: CREATING A DEVICE TEMPLATE FOR DNS SETTINGS
In this example, you create a template that configures the IP addresses of primary and secondary DNS servers.
1. In the navigation tree, select Device Manager > Security Device Templates. Click the Add icon in the Device Template Tree or the Device Template List.

The New Device Template dialog box appears, displaying the template navigation tree in the left pane and the Info screen in the right pane.

2. In the Info screen, enter DNS in the Name field.

3. From the template navigation tree, select Network > DNS. Configure the following:

   - For Primary DNS Server IP, enter 1.1.1.1.
   - For Secondary DNS Server IP, enter 2.2.2.2.
   - For DNS Refresh Schedule, select Refresh Daily. Leave all other default settings.

4. Click OK to save the template. You can now use this template when configuring security devices.

EXAMPLE: APPLYING A DEVICE TEMPLATE
In this example, you apply the DNS template you created in the previous example:

1. Ensure that the device you want to apply the template to has been successfully added to the management system.

2. In the navigation tree, select Device Manager > Security Devices, then double-click the device to open the Device dialog box.

3. In the device navigation tree, select Info > Templates. The templates configuration screen appears.

4. Click the Edit icon. The Edit Templates dialog box appears.

5. Select the DNS template.

6. Click OK in the Edit Templates dialog box, then click OK to save your changes to the device configuration.
The Template Operations Dialog

Template Operations Dialog Controls
The Template Operations dialog is divided into the following four sections:

Select Devices section
In this section, select one or more devices for template operations.

Select Template section
Select one or more templates to apply to the selected devices. Use the edit button to bring up the Select Templates dialog. Check one or more checkboxes to select templates. Once you have selected templates and closed the Select Templates dialog, use the up and down arrow buttons to order the selected templates as you wish.
Template Operation section

The next section features four radio buttons, as follows:

- **Add templates with lowest priority**—Adds the templates to each device’s template list with the lowest priority. Added templates will be lower priority than templates previously assigned to the device. Templates with higher priority can override the values applied by these templates.

- **Add templates with highest priority**—Adds the templates to each device’s template list with highest priority. Added templates will be higher priority than templates previously assigned to the device. Values in these templates will override values applied by lower priority templates.

- **Remove templates**—Removes all selected templates from each selected device.

- **Don’t change templates**—Makes no changes to devices in database. This setting is useful if you want perform a validation, run a report, or clear overrides without changing the template assignments.
Options section
The last section provides optional operations, as follows:

- **Remove conflicting device values**—overrides any device settings that override template values provided by the selected templates. Normally, template values do not override manually set values.

- **Report irrelevant template values**—reports any values that are set in templates but that are not used on the selected devices. A template may provide values for features that aren't available on every device. For example, wireless configuration information is not relevant to devices that do not provide wireless functionality.

---

NOTE: If the template specifies a field that a device does not support, the field does not appear in the Device dialog box and is not applied to the device. No validation message appears. You can see these values by checking the Report irrelevant template values checkbox.

If the template specifies a field that the device supports, but the value is outside the permitted range for the device, a validation message appears in the Device dialog box.

- **Report conflicts with other templates**—reports any values that conflict between the selected templates and existing templates assigned to the device. If there are undesired conflicts, you may need to modify the templates to get the configuration you want.

- **Validate**—checks that the configured device (after any changes) is a valid configuration and reports any errors.

Using the Template Operations Dialog
The Template Operations dialog allows you to add templates to devices, remove templates from devices, and validate device configurations after any changes.

---

NOTE: The Template Operations Dialog only updates the configuration database. To apply changes to devices, you must use the update directive.

The Template Operations dialog can be used in many ways. This section describes one recommended workflow.

Step 1: Look at the effect of planned changes before making them
1. Select Devices > Configuration > Template Operations.
2. Select one or more devices to validate templates against. Example: 5gt, 5gt-12, 5gt-13, 500, 520, 1000
3. Select the Edit Templates button to bring up a list of templates.
4. Select one or more templates to validate against the devices. Example: VPN, DNS, Route-Basic, Zone-Basic, admin-1
5. Click OK.

6. If you have selected more than one template, use the up and down arrow buttons to sort the templates. Templates higher in the list will be assigned first. Templates lower in the list will be assigned later. Later templates can override the settings of earlier templates.

7. Select the Don’t change templates radio button.

8. If you want, you can select one or more of the following validation and reporting options.

   - Report irrelevant template values (optional)—reports template settings that are not relevant to the selected device or devices.
   - Report conflicts with other templates (optional)—reports settings that conflict between two or more templates.
   - Validate (recommended)—validates the device configuration after appropriate changes to the templates and the removal of conflicting values (if needed).
   - Do not select Remove conflicting device values as it may alter device values.

9. Click OK.

Step 2: Review results in job information dialog

Figure 27: Template Operations Job Information Dialog
Consult the reports and error messages generated in Step 1. Resolve any conflicts, missing assignments, or other errors as desired. If desired, repeat steps 1 and 2 until you are satisfied with your planned changes.

Step 3: Apply templates and clear overrides
This procedure updates the NetScreen-Security Manager database, but does not push the new settings to the device.

CAUTION: You can easily reverse adding templates, but there is no automatic way to restore conflicting device values that have been removed. Be careful not to override values you want to keep.

Repeat the operations specified in Step 1, but specify one of the Add templates radio buttons. If desired, also check the Remove conflicting device values checkbox.

Removing Templates with the Template Operations Dialog
To remove one or more templates from one or more devices, select Devices > Configuration > Template Operations.

1. Select one or more devices to remove templates from.
   Example: 5gt
2. Select the Edit Templates button to bring up a list of templates.
3. Select one or more templates to remove.
   Example: DNS
4. Click OK.
5. Select the Remove templates radio button.
6. Click OK.

Templates and Validation
You can apply a single template to different device types that run different ScreenOS versions. In some cases, the field values you specify in the template might not be appropriate for all ScreenOS versions and device types:

- If the template specifies a field that a device does not support, the field does not appear in the Device Edit dialog box and is not updated to the device. No validation message appears.

- If the template specifies a field that the device supports, but the value is outside the permitted range for the device, a validation message appears in the Device dialog box. A template value may be valid for one device but invalid for other devices.
As you create and edit template values and fields, NetScreen-Security Manager performs validation, and might display validation messages. For example, you can configure an IP address in one template and the netmask for that IP address in another template. However, a validation message might appear when you enter the IP address because the netmask is not specified within that same template.

You can safely ignore a validation message if the missing value is derived from another template that is applied to the device, or if you manually entered in the value in the specific device configuration.

**Modifying Template Values**

You can modify a template that has already been applied to one or more device configurations. When you change a field value in a template, the new value appears in the device configuration the next time you edit the configuration. To change the field value on the device, you must update the device (see Chapter 6, “Updating Devices”).

When you change a template, the configuration of one or more devices that use the template might become invalid. For example, a template change could cause a required field to be cleared or a field value to be outside the permitted range.

For step-by-step instructions on modifying a template, see the NetScreen-Security Manager Online Help topic, “Editing Device Template”.

**Applying Multiple Templates**

When applying multiple templates to a single device, you determine the order that the templates are applied. The highest priority template is positioned at the end of the template list, and can override values set in any of the lower priority templates. If more than one template specifies a value for the same field, the value in the highest-priority template takes precedence. The lower the template appears in the template list, the higher priority it has when applying values to a device configuration.

**EXAMPLE: USING MULTIPLE DEVICE TEMPLATES**

In this example, you create two templates that each configure different values for the same firewall SCREEN option for the untrust zone. The first template, DoS, sets several values in the SCREEN options, including setting the source-based IP session threshold limit to 128 for the untrust zone. The second template, DoS2, sets the source-based IP session threshold limit to 256 for the untrust zone. When you apply these templates to a device, the template with the highest priority overrides the values in the lower priority template.

1. Create a template that sets SCREEN options for the untrust zone then apply the template to a NetScreen-208 device running Screen 4.0:

   a. In the navigation tree, select Device Manager > Security Device Templates and click the Add icon. The New Device Template dialog box appears.

   b. In the Info screen, enter **DoS** in the Name field.

   c. In the template navigation tree, select Network > Zone. The Zone configuration screen appears.
d. Click the Add icon in the Zone configuration screen and select Predefined Security Zone. The Predefined Zone dialog box appears.

NOTE: Because the untrust security zone is predefined for the device, you must select the Predefined Security Zone option. You can select the Security Zone or Tunnel Zone option only when adding or configuring a user-defined zone.

e. In the General Properties screen, enter **untrust** in the Name field.

f. In the zone navigation tree, select Screen > Denial of Service Defense. The Denial of Service Defense screen appears.

g. Select and configure the following options, then click OK:

- Select SYN-ACK-ACK Proxy Protection and set the Threshold to 512.
- Select Source IP Based Session Limit and set the Threshold to 128.
- Select Destination IP Based Session Limit and set the Threshold to 4000.

h. Click OK to save the new device template.

2. Apply the DoS template to a device configuration for a NetScreen-208 running ScreenOS 4.0:

a. Add a NetScreen-208 security device to the management system, and model the configuration. Be sure to configure the device as running ScreenOS 4.0.

b. In the navigation tree, select Device Manager > Security Devices. Double-click the NetScreen-208 device icon to open the Device dialog box.

c. Select Info > Templates in the device navigation tree. Click the Edit icon in the Templates screen. The Edit Templates dialog box appears.

d. Select the DoS template.

e. Click OK in the Edit Templates dialog box.

3. Verify that the DoS template values have been applied to the device:

a. Select Network > Zone in the device navigation tree. Double-click the untrust zone. The untrust-Predefined Zone dialog box appears.

b. Select Screen > Denial of Service Defense and review the values applied by the template, as shown below:
4. Create a second template that sets a different value for a SCREEN option than was set in the DoS template:

   a. In the navigation tree, select Device Manager > Security Device Templates and click the Add icon. The New Device Template dialog box appears.

   b. In the Info screen, enter **DoS2** in the Name field.

   c. In the template navigation tree, select Network > Zone. The Zone configuration screen appears.

   d. Click the Add icon in the Zone configuration screen and select Predefined Security Zone. The Predefined Zone dialog box appears.

   e. In the General Properties screen, enter **untrust** in the Name field.

   f. In the zone navigation tree, select Screen > Denial of Service Defense. The Denial of Service Defense screen appears. Select and set the Source IP Based Session Limit Threshold to 128.

   Your settings appear as shown below:

   ![Denial of Service Defense Configuration](image)

   Because the NetScreen-208 is running ScreenOS 4.0, the Destination IP-Based Session Limit does not appear (this option is not supported by ScreenOS 4.0.x) and is not applied to the device.
g. Click OK in the Predefined Zone dialog box, then click OK in the New Device Template configuration dialog box.

5. Apply the DoS2 template to the NetScreen-208 device:

a. In the navigation tree, select Device Manager > Security Devices. Double-click the NetScreen-208 device icon to open the Device dialog box.

b. Select Info > Templates in the device navigation tree. Click the Edit icon in the Templates configuration screen. The Edit Templates dialog box appears.

c. Select the DoS2 template.

d. Click OK in the Edit Templates dialog box.

6. Set the template priority.

Currently, the DoS template has the highest priority, which enables it to override any similar values set by the DoS2 template, as shown below:

Figure 30: View Template Priority (DoS Highest)

To set the DoS2 template to the highest priority, select the DoS2 template and click the down arrow icon above the list of templates (or press Alt-N.) The DoS2 template now has the highest priority, as shown below:
Chapter 5: Configuring Devices

Figure 31: Set Template Priority (DoS2 Highest)

The DoS2 template now overrides similar values set in the DoS template.

7. Verify that the configuration values from the DoS and DoS2 templates have been applied in the device configuration:

   a. Select Network > Zone in the device navigation tree. Double-click the untrust zone. The untrust-Predefined Zone dialog box appears.

   b. Select Screen > Denial of Service Defense and review the values applied by the template, as shown below:

Figure 32: View Values from DoS and DoS2 Templates

Although both the DoS and DoS2 templates configured threshold values for the Source IP Based Session Limit field, the higher threshold value from DoS2 appears in the device configuration because you assigned the DoS2 template a higher priority than the DoS template.

   c. Verify the origin of each value by pressing the Shift key and moving the mouse cursor over the field name.

For the Source IP Based Session Limit, the message “From template: DoS2” appears, as shown below:
Using Device Groups

Use device groups to organize your managed devices, making it easier for you to configure and manage devices within a domain. You can group devices by type (such as all the NetScreen-5GTs in a domain), by physical location (such as all the security devices in the San Jose office), or logically (such as all the security devices in sales offices throughout western Europe.)

Groups enable you to execute certain NetScreen-Security Manager operations on multiple security devices at the same time. For example, if you have a group of the same type of devices running similar ScreenOS versions, you can upload the firmware on all devices in the group at the same time. You can also add devices to the NetScreen-Security Manager UI, place the devices in a group, and then import the device configurations for all devices in the group at one time.
The devices that you add to a group must exist; that is, you must have previously added or modeled the devices in the domain. You can group devices before configuring them. You can add a device to more than one group. You can also add a group to another group.

NOTE: You cannot apply a template to a group. You must apply templates to individual devices in a group. If you need to apply the same set of templates to multiple devices, you can create a single template that includes all the templates that are to be applied to a device, and then apply the combined template to each device.

EXAMPLE: CREATING A DEVICE GROUP
In this example, you create a device group that includes security devices used to protect the Sales and Marketing department of your organization.

1. Add and model the following devices to the management system:
   - Outside Sales
   - Marcom
   - Direct Marketing
   - Sales
   - Marketing
2. In the navigation tree, select Device Manager > Security Devices.
3. Click the Add icon. The New Group dialog box appears, displaying all existing devices for the current domain in the Non-members list.
4. For Name, enter Sales.
5. In the non-members list, select the devices that you want to be part of the Sales device group.
6. Click Add=> to move the selected devices to the Member list. Click OK.

Configuring Device Information

To configure a device that has been added, imported, or modeled in NetScreen-Security Manager:

1. In the navigation tree, select Device Manager > Security Devices.
2. Open the device configuration using one of the following methods:
   - Double-click the device object in the security device Tree or the security device List.
   - Select the device object and then click the Edit icon.
   - Right-click the device object and select Edit.
The device navigation tree appears on the left, listing the device configuration parameters by function.

3. In the device navigation tree, select a function heading to see device parameters, then select the configuration parameter you want to configure.

4. Make your changes to the device configuration, then choose one of the following:
   - Click OK to save your changes and close the device configuration.
   - Click Apply to save your changes and continue making changes.
   - Click Cancel to discard all changes and close the device configuration.

This section describes the Info options in the Device dialog box. Subsequent sections describe other options in the Device dialog box.

When you add or model a device in the NetScreen-Security Manager UI, you provide information about the device name, color, type, and OS version. If you imported the device configuration, the Info options display additional information about the device:

- **Info**—specifies the device name and the color that you have chosen to display the device in the NetScreen-Security Manager UI.

- **Device Type**—specifies the type of security device that you are managing, including the version of ScreenOS that you are running on the device. Note that two types of OS Version now appear on the device:
  - **Managed OS Version** refers to the version of ScreenOS that is supported by NetScreen-Security Manager
  - **Running OS Version** refers to the actual version of ScreenOS running on the device - this may be a future version of ScreenOS not yet fully supported by NetScreen-Security Manager

Support Level indicates whether or not features on the device are either “Fully Supported” in which case you can use NetScreen-Security Manager to manage all the functionality in that version of ScreenOS, or “Forward Supported”, in which case you can use the Supplemental CLI to facilitate support of new features in ScreenOS. For more details on using Supplemental CLI, refer to “Configuring Supplemental Command Line Interface (CLI)” on page 346.

Other information including the Serial Number, IP Address and whether or not you are running the device in Transparent Mode is also provided:

- **Device Root Admin**—specifies the username and password of the root admin on the device

- **NSM Connection**—specifies the type of connection that NetScreen-Security Manager is using to connect to the device.

- **Policy for Device**—specifies the name of the policy that you are using to configure traffic on the device.
Configuring Startup Information

For modeled devices, and for imported devices that use a dynamic IP address, you must configure Startup information. The startup information includes the One-Time-Password (OTP) and the Device Server parameters.

NOTE: Certain encrypted passwords/keys are not imported into NetScreen-Security Manager including the OTP, root admin password, and wireless ssid psk-key and passphrase. If any of the above passwords/keys are changed out of band, then you must copy and save the encrypted value of the password/key using NetScreen-Security Manager. This enables you to avoid resetting the previous configured value upon next update. Other passwords and keys such as the “non-root admin” passwords are imported into NetScreen-Security Manager.

The OTP is used to authenticate the first connection communication between the physical device and NetScreen-Security Manager. The OTP is deactivated (unavailable) when:

- You have already set the OTP. After you have configured an OTP, you cannot reset it.
- For imported devices that use a static IP address. Because first connection communication occurs during the add device process, the OTP is not used and is deactivated by default.
- For devices running ScreenOS 4.x. These devices do not use an OTP

Use the Device Server parameters to specify the primary and, if available, the secondary Device Server IP addresses and ports that manage the security device.

Applying Templates

You can set most device configurations, except policies and VPNs, in a template. You can also manually override any value set by a template.

The order in which the templates are listed determines how template values are applied to the device. When a value is set in more than one template applied to a device, the value in the highest-priority template takes precedence. To reorder templates, click the up or down arrow icon above the list of templates to move the priority up (lower priority) or down (higher priority). (Or, press Alt-U or Alt-N to move the priority of the template up or down.)

For more information about templates, see “Using Templates” on page 133.

Viewing Device Capabilities

The Capabilities screen lists features and resources available on the device. This screen is read-only; you cannot change any of the values on the screen.

The configuration screens that you see for a particular security device depend upon the following:

- Device platform
ScreenOS version running on the device
License key(s) installed on the device

Therefore, some of the configurations described in this chapter only apply to specific security devices, ScreenOS versions, or license key installations.

Configuring Network Overview

The Network screens contain the options that enable the device to connect to and operate in the network. In the Device navigation tree, open the Network heading in the navigation tree to see the network settings options.

The following sections detail configuring the following network settings:

- Configuring Wireless Settings. This option is available only for NetScreen-5GT Wireless security devices running ScreenOS 5.0.0-WLAN; this device can act as a wireless access point (WAP). The wireless settings specify how the WAP connects multiple wireless networks or a wireless network to a wired network.

- Configuring the Network Module (Slot and Chassis). This option is only available for security device systems, such as the NetScreen-5000 series, ISG 1000/2000, and SSG 520/550, that contain a motherboard or physical slots in which you can install optional modules. You can view or edit the type of network module installed in each available slot in the physical device.

- Configuring Virtual Routers. A virtual router (VR) supports static routes, dynamic routing protocols, and multicast protocols. The virtual router configuration includes the configuration for dynamic routing protocols and multicast protocols.

- Configuring Zones. A security zone is a specific network segment for which you can control inbound and outbound traffic. You can configure predefined zones or create user-defined security zones. You can also create a tunnel zone, which is a logical segment to which a VPN tunnel interface is bound.

- Configuring Interfaces. You bind interfaces to predefined or user-defined security zones or to tunnel zones to permit traffic to pass into or out of the zone. For an interface in Route or NAT mode, you assign an IP address to the interface.

- Configuring DIP Groups. You can configure a range of IP addresses from which security device can take addresses when performing network address translation (NAT) on the source IP address of outgoing or incoming IP packets.

- Configuring PPPoE. This option is only available for some security devices. You can configure PPPoE to enable the security device to connect to remote sites.

- Configuring PPP. This option is only available for some security devices. You can configure PPP to enable the security device to connect to remote sites.
Configuring Wireless Settings

The wireless settings specify how a wireless-capable security device connects multiple wireless networks or a wireless network to a wired network. You can configure wireless settings only on a Juniper Networks NetScreen-5GT Wireless security device running ScreenOS 5.0.0-WLAN or ScreenOS 5.0.0-DSLW; these devices can act as a wireless access point (WAP).

When you deploy a NetScreen-5GT Wireless as a WAP, the security device manages a distribution system of one to eight basic service sets (BSSs). Each BSS uses a unique name identifier, called a service set identifier (SSID). Each host within a BSS must have the same SSID as that configured for that BSS on the security device. When configuring the SSID, you bind each BSS to its own interface (and zone); segmenting BSSs enables you to enforce different levels of device authentication and encryption for each zone, and to create rules that control wireless traffic across zones.

NOTE: When security zones contain wireless and wired networks, they must use separate subnets and connect to the device through different interfaces with logically separate IP addresses.

The NetScreen-5GT Wireless security device supports up to 60 wireless clients concurrently.
Configuring General Wireless Settings

NetScreen-5GT Wireless security device contains a radio transmitter/receiver with a frequency range of 2.4GHz to 2.4835GHz, and supports the IEEE 802.11b and 802.11g standards. When you first deploy the NetScreen-5GT Wireless device on your network, the radio transmitter/receiver is configured with default settings designed to work in most networking environments.

You can edit the default values for the following radio settings:

- Antenna settings
- Channel settings
- Operation Mode settings
- Transmission Power and Rate settings

The following sections detail each radio setting.

Configuring Antennas

You can use one antenna or a pair of antennas on the NetScreen-5GT Wireless security device. Select the antenna option that meets your network needs and that corresponds to the actual physical antenna configuration on the device.

To configure the antenna, in the device navigation tree, select Wireless Settings then select one of the antenna configurations:

- Diversity antennas—Select this option when the security device is using a pair of diversity antennas that provide 2dBi omnidirectional coverage (signal radiates 360 degrees horizontally). These antennas provide a fairly uniform level of signal strength within the area of coverage and are suitable for most installations (diversity antennas ship with the NetScreen-5GT Wireless device). This is the default option.
Antenna A or Antenna B—Select one of these options when using a single antenna for 2dBi omnidirectional coverage (signal radiates 360 degrees horizontally). Unlike diversity antennas, which function as a pair, the external antenna operates singly to eliminate an echo effect that can sometimes occur from slight delay characteristics in signal reception when two antennas are in use.

NOTE: On the NetScreen-5GT Wireless security device, antenna A is nearest the power connector port.

When importing wireless settings from a security device, NetScreen-Security Manager automatically displays the antenna settings configured on the physical device. Before activating a modeled wireless security device, however, you must ensure that the antenna setting you select in the NetScreen-Security Manager UI matches the actual antenna configuration on the physical device. For example, if you model the device using antenna A as a single antenna providing 2dBi omnidirectional coverage, you or the device administrator must have connected an antenna to antenna port A on the physical device before you activate that device.

Configuring Channels

The wireless security device uses channels to send and receive wireless traffic. The device uses the same channel for all basic service sets (BSSs), which share the same overall bandwidth, and distinguishes traffic from different BSSs by the SSID number.

By default, the wireless security device automatically selects the appropriate channel based on the country code. To select a specific channel, in the device navigation tree, select Wireless Settings and change the Channel for Wireless AP Radio setting to Channel Number, then enter the channel number you want the device to use. To enable the device to use additional channels that might be available in your country, select Extended Channel Mode.

The regulatory domain for channel assignments is not configurable, and is preset as one of the following:

- **FCC (USA)**—This regulatory domain automatically sets the country code to USA. Because you cannot change this setting, it does not appear in the UI.

- **TELEC (Japan)**—This regulatory domain automatically sets the country code to Japan; you cannot change this setting. Because you cannot change this setting, it does not appear in the UI.

- **WORLD (all countries)**. This regulatory domain requires you to select from a list of countries (can select USA or Japan). If the device is preset to use FCC or TELEC, this setting does not appear in the UI.

NOTE: Although you can select the Extended Channel Mode option when the regulatory domain is WORLD and the selected country code is USA, there are no extended channels in the USA.
Configuring Operation Mode Settings
The NetScreen-5GT Wireless supports both 802.11b and 802.11g operation modes, either simultaneously (default setting) or exclusively. To configure the operation mode, in the device navigation tree, select Wireless Settings then select one of the following modes:

- To enable both 802.11b and 802.11g wireless clients to connect to the wireless security device, select 802.11b/g.

**NOTE:** We recommend you enable CTS protection (see “Configuring Control Frame Protection” on page 158) to avoid collisions when supporting 802.11b and 802.11g operation modes.

- To enable only 802.11b wireless clients to connect to the wireless security device, select 802.11b.

- To enable only 802.11g wireless clients to connect to the wireless security device, select 802.11b/g, then select the checkbox for 802.11g Only.

Configuring Transmission Settings
Use the transmission settings to control the power and rate used by the wireless interfaces. To configure the transmission settings, in the device navigation tree, select Wireless Settings, then edit the default values for the following settings:

- Transmit Power—This setting controls the power transmission and radio range. By default, the power level is set to full; available settings include an eighth, half, minimum, or quarter. You might need to edit this setting when using more than one wireless interface in the same location and frequency.

- Data Rate for AP—This setting controls the wireless interface data transmission rate for sending frames. By default, the rate is set to best rate (the wireless interface uses the best rate first, and then automatically falls back to the next rate if transmission fails).
  - For 11b transmissions, available rates are 1, 2, 5.5, and 11 mbps.
  - For 11g transmissions, available rates are 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 mbps.

Configuring Advanced Wireless Settings
Use the advanced wireless settings to control low-level wireless networking settings, such as aging values and collision protection. When you first deploy the NetScreen-5GT Wireless device on your network, the network settings are already configured with default settings designed to work in most networking environments. However, you might want to edit these settings to meet your specific wireless networking needs.

You can edit the default values for the following wireless networking settings.
Configuring Aging
The aging interval is the amount of time (in seconds) that a wireless client or bridge remembers an access point after communication with the WAP is lost. To configure the aging setting, in the device navigation tree, select Wireless Settings > Advanced, then edit the default aging value.

The default is 300 seconds; acceptable range is 60 to 1,000,000 seconds. To disable aging, set the value to 0 (zero).

Configuring Beacons
A WAP broadcasts beacon packets to keep the wireless network synchronized and to inform wireless clients of waiting data. A beacon packet includes data such as the wireless LAN service area, the WAP address, and Delivery Traffic Indicator Maps (DTIMs).

To configure the beacon settings, in the device navigation tree, select Wireless Settings > Advanced, then edit the default values for the following settings:

- Beacon Interval—The beacon interval is the amount of time between beacons sent by the NetScreen-5GT Wireless to wireless clients. A beacon transmission includes the beacon interval; the interval informs receiving devices how long they can wait in low-power mode before waking up to handle beacons. Increasing the beacon interval lessens the number of beacon responses required by a wireless client, enabling clients to reduce battery power. The default value is 100 time units; acceptable range is 20 to 1,000 time units (1 time unit equals 1024 µs).

- Beacon Interval Between DTIMs—This interval is the amount of beacon intervals between Delivery Traffic Indicator Map (DTIM) messages, which inform wireless clients of waiting data. A lower value enables wireless clients to download waiting data more often; a higher value enables wireless clients to wait in low-power mode longer between DTIMs. When using a high DTIM value however, the client must stay active longer to collect waiting data, and clients might miss broadcast and multicast traffic messages. The default value is 1 beacon interval; acceptable range is 1 to 255.

Configuring Burst and Fragment Size
Use the burst and fragment setting to configure how the device transmits wireless packets over the network. To configure the burst and fragment settings, in the device navigation tree, select Wireless Settings > Advanced, then edit the default values for the following settings:

- Maximum Number of Frames in a Burst—The burst threshold defines the average maximum number of frames a WAP can use to handle wireless traffic before the device begins sending traffic in bursts. When wireless traffic exceeds the specified threshold, the device sends wireless packets in bursts to clients, who can switch to a low-power sleep state between bursts. The default value is 3 frames; acceptable range is 2 to 255 frames.
- **Fragmentation Threshold**—The fragmentation threshold defines the maximum size of a packet that can be transmitted without fragmentation. If the packet size exceeds the specified threshold, the sender (client or WAP) must fragment the packet before transmitting.

  Using a high fragmentation threshold reduces the number of fragments on the wireless network, which can increase efficiency. However, large, unfragmented packets can be corrupted during transmission, requiring resend attempts that can decrease efficiency. The default value is 2346; acceptable range is even numbers between 256 and 2346.

### Configuring Control Frame Protection

Control frame protection is designed to help avoid collisions on the wireless network. Transmission collision usually occurs when two wireless devices are within range of the same WAP, but are not within range of each other (they are hidden nodes). If two wireless transmissions collide at the WAP, the data in each transmission is lost.

To avoid collisions, you can require wireless clients to first request permission to send data (clients must send a request-for-send (RTS) frame) and/or receive approval of that request (client must receive a clear-to-send (CTS) frame) before transmitting data.

Because 802.11b stations can't hear 802.11g stations using Orthogonal Frequency Division Multiplexing (OFDM), a method for wireless transmission that divides a signal and transmits the pieces at different frequencies simultaneously, traffic from these stations can collide on the network, reducing network efficiency. We recommend you enable protection to avoid collisions when supporting 802.11b and 802.11g operation modes.

**NOTE:** CTS protection is not supported when using 802.11b only.

To configure the control frame protection settings, in the device navigation tree, select Wireless Settings > Advanced, then edit the default values for the following settings:

- **Threshold for RTS to Transmit**—The request-to-send (RTS) threshold defines the maximum size of a packet that a wireless client can send without obtaining permission from the WAP. If a packet exceeds this threshold, the client must send an RTS message to the WAP requesting permission to send the packet. You might want to adjust this setting to control traffic flow through an access point that services a large number of clients. The default is 2346; accepted range is 256 to 2346.

- **CTS Protection Mode**—Enables Clear to Send (CTS) control frame protection, which requires wireless client to first receive a CTS frame from the WAP before sending data. Select one of the following protection modes:
  - **On**—When selected, wireless clients must first receive a CTS frame from the device before sending data.
  - **Off**—When selected, wireless clients do not send CTS control frames.
- **Auto**—When selected, the device automatically detects the CTS mode used by the wireless client. This is the default setting.

- **CTS Protection Type**—The protection type defines the level of control frame protection enforced by the device. Select one of the following protection types:
  - **CTS Only**—When selected, wireless clients must first receive a single, self-directed CTS frame from the device before sending data. This is the default setting.
  - **CTS-RTS**—When selected, wireless clients must first send an RTS frame and receive a CTS frame from the device before sending data (a two-frame exchange occurs prior to the actual network transmission).

- **CTS Rate**—The CTS rate defines the data rate (in Mbps) at which CTS frames are sent. The default rate is 11 Mbps, acceptable values are 1, 2, 5.5, and 11.

### Configuring Short Slots

Short slots, an 802.11g-only feature, can increase efficiency and throughput for wireless traffic. By default, the device supports 802.11g traffic that uses short slots. However, because 802.11b does not support short slots, you might want to disable short slots for all protocols when your wireless network is handling 802.11b traffic.

To disable short slot for 802.11g packets, in the device navigation tree, select **Wireless Settings > Advanced**, then select **Set Slot Time to Long**.

### Configuring Preambles

A preamble is the sequence of bits within a transmission that, when recognized and received by a wireless client, enables the client to locate the remaining packets in the transmission. The preamble length is defined in the Synchronization field of a wireless packet, and can be long or short:

- A long preamble (128 bits) provides the wireless client more time to process the preamble, which can provide greater interoperability with older wireless protocols and non-short-preamble equipment. All 802.11 devices support a long preamble.

- A short preamble (56 bits) can improve efficiency because the client does not spend time processing the preamble. However, older wireless protocols do not support short preambles.

By default, the device does not support long preambles. To enable long preambles for 802.11b packets only, in the device navigation tree, select **Wireless Settings > Advanced**, then select **Long Transmit Preamble**.

### Configuring Wireless MAC Access Lists

The access control list (ACL) controls the wireless clients that can connect to the wireless network. The ACL identifies clients by their MAC addresses and directs the device to permit or deny access for each address. The ACL settings apply globally to all basic service sets (BSSs).
Configuring MAC Access Mode

You can configure the ACL to operate in one of the following modes:

- **Disabled**—When enabled, the security device does not filter MAC addresses. This is the default mode.
- **Enabled**—When enabled, the security device permits access to all hosts except those marked with a Deny control status. Use this option when you want to deny specific hosts, but allow unknown hosts to connect.
- **Strict**—When enabled, the security device denies access to all hosts except those marked with an Allow control status. Use this option when you want to restrict network access to specific hosts.

To configure the ACL mode, in the device navigation tree, select Wireless Settings > MAC Access List, then select the MAC Access Mode.

Configuring MAC Addresses

You can specify a maximum of 128 MAC addresses. To add an address, in the device navigation tree, select Wireless Settings > MAC Access List, then click the Add icon to display the New MAC address dialog box. Configure the following:

- **MAC Address**—Defines the MAC address of the client.
- **Control Status**—The control status defines the action the device takes when a client with the specified MAC address is detected.

  For example:

  - If the control status is set to Deny and the MAC access mode is set to Strict, the device denies the client.
  - If the control status is set to Allow and the MAC access mode is Deny or Strict, the device allows the client to connect.

  **NOTE:** NetScreen-Security Manager does not support the learned MAC address list.

Configuring Wireless SSIDs

To enable wireless clients to connect to the NetScreen-5GT Wireless security device, you must configure at least one basic service set (BSS) that defines and controls how the device handles traffic through a wireless interface.

You can create up to eight basic service sets, but the device can only use a maximum of only four at one time. You might want to configure extra service sets when your network uses site-specific or time-specific BSSs—to enable different BSSs, bind or unbind their corresponding SSIDs to interfaces.
Configuring General SSID Settings

A new SSID does not contain default general settings; you must at least configure a name and select wireless interface for the SSID before the device can handle wireless traffic for that BSS.

- **Name**—The name uniquely identifies the BSS. The device uses the SSID name to distinguish the interface to route wireless traffic to. For enhanced security, do not assign the SSID a meaningful name that an attacker might be able to determine through reconnaissance, such as the department or location of the WAP. You can also make the name difficult to guess by using a mix of upper- and lowercase letters, numbers, and symbols. When the SSID name contains one or more spaces, enclose the name within quotation marks.

- **Suppressing Transmission of SSID Information**—When enabled, the device does not display the SSID name in broadcasts. Because the name is not broadcast, attackers must work harder to obtain the SSID name.

- **Isolation of Clients on the Same SSID**—When enabled, prevents wireless clients on the same subnetwork (SSID) from communicating directly with each other and bypassing the security device.

- **Wireless Interface**—Select the wireless interface (wireless 1 or wireless 2) that handles traffic for the SSID. The device routes all wireless traffic with the specified SSID name through this interface.

Configuring SSID Authentication and Encryption

Each SSID can use specific authentication and encryption settings, enabling you to configure differing levels of security for different resources. By default, the authentication/encryption is set to none; we strongly recommend that you select one of the supported authentication/encryption methods. The NetScreen-5GT Wireless device supports WEP and WPA authentication and encryption methods; to ensure the highest level of security we recommend that you select WPA as your authentication/encryption method.

The Wired Equivalent Privacy (WEP) uses the Rivest Cipher 4 (RC4) stream cipher algorithm to encrypt and decrypt data as it travels over the wireless link. You can store WEP keys locally on the security device or externally on an external authentication server. Wireless network users store one or more of the same keys on their systems and identify them with the same ID numbers. For details on configuring WEP, see “Configuring Wired Equivalent Privacy (WEP)” on page 162.

The Wi-Fi Protected Access (WPA) method patches many of the security vulnerabilities found in WEP, greatly enhancing payload integrity checks and the key exchange process. You can use WPA in one of the following modes:
WPA Mode—In this mode, also known as Enterprise Mode, the device uses the Extensible Authentication Protocol (EAP) for authentication through a 802.1X-compliant RADIUS server (such as the Funk Odyssey RADIUS server and the Microsoft IAS RADIUS server). When handling wireless traffic, the device forwards authentication requests and replies between the wireless clients and the RADIUS server; after successfully authenticating a client, the RADIUS server sends an encryption key to both the client and to the device. The device itself manages the encryption process using Temporal Key Integrity Protocol (TKIP) or Advanced Encryption Standard (AES).

WPA-PSK—In this mode, also known as Personal Mode, the device uses preshared keys (Preshared Key = PSK) or passphrase for authentication and encryption. Keys are stored on the device and on all wireless clients; you do not need to configure a separate authentication server.

For details on configuring WPA, see “Using Wi-Fi Protected Access (WPA)” on page 165.

Configuring Wired Equivalent Privacy (WEP)
Although you can configure WEP for all the basic service sets (BSSs), the NetScreen-5GT Wireless (ADSL) device intentionally restricts its use to only one BSS at a time.

Auto—When selected, the device automatically negotiates with wireless clients whether or not the client authenticates itself with a WEP shared key (device accepts both open encryption or shared-key authentication). Use this option to improve compatibility between the WAP and wireless devices using various operating systems that support different implementations of WEP.

Open—When selected, a wireless client must provide the SSID to the device before the device authenticates the client. For encryption, select one of the following:

- None—When selected, no encryption is performed.
- WEP—When enabled, an authenticated wireless client must provide a WEP key to the device before the client can encrypt and decrypt communication over the WLAN. Because the Open option is insecure (especially if the device is configured to broadcast the SSID), we recommend that you also enable WEP encryption.

When using WEP encryption, you must also select a key source, which specifies the location of the WEP key:

- None or Local—The key is stored on the security device. This is the default key-source when None is selected. When enabled, you must configure a default WEP key on the security device.
Server—The key is stored on a RADIUS authentication server. When enabled, you must configure a RADIUS authentication server to handle WEP key requests (you do not need to configure or use a WEP key on the security device).

Both—The key is stored on the security device and on the RADIUS authentication server. When enabled, you must configure a RADIUS authentication server to handle WEP key requests and configure a default WEP key on the security device.

Shared Key—When selected, both the device and the wireless clients use the same key for authentication and encryption/decryption. You must configure a default WEP key on the security device.

During a shared key exchange:

a. The wireless client contacts the device.

b. The device responds to the client with a clear-text challenge text string that the client must then encrypt with the correct WEP key and return to the device.

c. The device receives the encrypted string from the client, decrypts it, and compares it with the original. If the strings match, authentication is successful; if the strings do not match or the client does not respond, authentication fails.

Although this method uses WEP keys for encryption, an attacker might be able to intercept both the clear-text challenge and the same challenge encrypted with a WEP key, and potentially decipher the WEP key.

Configuring WEP Keys
You can define WEP keys on the security device for BSS use. The security device, acting as a wireless access point (WAP), uses WEP keys for authenticating wireless clients in that BSS, and for encrypting and decrypting traffic sent between itself and the clients.

You can define one to four WEP keys for each BSS on the security device. Using multiple keys enables you to adjust the level of security for different wireless clients within the same BSS; you can use longer keys to provide greater security for some traffic and smaller keys to reduce processing overhead for other, less critical traffic.

When you define only one WEP key on the security device, that key is the default key and handles all encryption, authentication, and decryption. When you define multiple keys on the security device, you can designate non-default keys to handle authentication and decryption (the default key always handles encryption). If you do not specify a default key, the first key you define automatically becomes the default key.

Wireless clients can use a static WEP key stored on the device, or a dynamic key on an external RADIUS server.
When clients use a unique, dynamic WEP key from an external RADIUS server, the security device also uses this unique key—which it also receives from the RADIUS server—for bidirectional communication.

When clients use static WEP keys stored locally on the security device, the device uses the default key to encrypt all transmitted wireless traffic. Clients must also have the default key loaded to decrypt traffic from the device.

Setting Key IDs
The Key ID enables WEP key configuration and sets the WEP identification value. When all WEP keys are stored on the security device, you can assign the default key ID as 1, 2, 3, or 4.

However:

- When using WEP keys stored on the security device and dynamic WEP keys created by an external RADIUS server (RADIUS dynamically creates and distributes a different key per session for each wireless client), the ID for the default WEP key on the security device cannot be 1 because the RADIUS server uses 1 as the ID for all its keys. The security device can use a default WEP key with key ID 2, 3, or 4 for encryption, and a different WEP key with ID 1, 2, 3, or 4 for authentication and decryption.

- When all WEP keys are on an external RADIUS server, the server uses a key ID of 1 for all its keys (RADIUS dynamically creates and distributes a different key per session for each wireless client).

Setting Encryption Length
An encryption key length specifies the length of the key in bits. Juniper Networks supports two WEP key lengths: 40 and 104 bits. Because the keys are concatenated with a 24-bit initialization vector (IV), the resulting lengths are 64 and 128 bits.

Longer keys are more secure than shorter keys, but longer keys take longer to process and can reduce throughput speeds. Select the key length that is appropriate to the importance of the wireless traffic you want to protect:

- 40-bit—A 40-bit encryption length enables you to enter 10 hexadecimal digits or 5 ASCII characters.
- 104-bit—A 104-bit encryption length enables you to enter 26 hexadecimal digits or 13 ASCII characters.

Setting the Encryption Method
The encryption method defines the string type (ASCII or Hexadecimal) for the WEP key:

- ASCII—Plain text string.
  - When using 40-bit length and ASCII method, enter 5 ASCII characters.
  - When using a 104-bit length and ASCII method, enter 13 ASCII characters.
**Hexadecimal (default)—**A hexadecimal string uses only A-F and characters and 0-9 numbers. For example, 662ADC918DDD662ADC918DDD66 is a valid hexadecimal string but CADETS01234567890123456789 is not; the T and S are outside the valid hexadecimal range. The number of hexadecimal characters you enter depends on the specified key length:

- When using 40-bit length and hexadecimal method, enter 10 hexadecimal characters.
- When using a 104-bit length and hexadecimal method, enter 26 hexadecimal characters.

**Setting the Default Key**

When using a single key on the security device for encryption, decryption, and authentication, you must define the default WEP key.

You can specify a static, non-default WEP key that the security device uses for authenticating and decrypting traffic received from wireless clients. However, each client must also load the WEP key (and ID) before they can authenticate themselves and send encrypted traffic to the security device. If a client does not supply a key ID, the security device attempts to use the default WEP key to authenticate the client and decrypt its traffic.

**Using Wi-Fi Protected Access (WPA)**

You can configure the SSID to use WPA enterprise mode or WPA personal mode:

- **WPA (Enterprise Mode)** authentication uses an external RADIUS auth server for authentication. When using WPA, you must also configure the rekey interface and encryption method:

  - **Encryption**—The encryption setting specifies the encryption method used between the security device and wireless clients in the subnetwork. Select one of the following:
    - **AES**—The American Encryption Standard (AES) is used by WPA 2 devices. AES uses the Robust Security Network (RSN) cipher for encryption. This complex encryption mechanism is a block cipher (operates on 128 bit data blocks).
    - **TKIP**—The temporal key integrity protocol (TKIP) is used by WPA 1 devices. TKIP is a key management protocol that handles key generation and key synchronization; TKIP uses the RC4 algorithm for encryption.
    - **Auto**—When enabled, the device uses the encryption method (AES or TKIP) used by the client.

  - **rekey-interval**—The rekey interval defines the number of seconds between group key updates. To enable key updates, select Value; the default interval is 1800 seconds and the acceptable range is 30-42949672 seconds. To disable key updates, select Disabled.
- WPA-PSK (Personal Mode) authentication uses a passphrase or pre-shared key on the security device to permit access to the SSID. When using WPA, you must also configure the WPA-PSK authentication and encryption method:

- Authentication (WSA-PSK)—Specifies the authentication options for wireless clients attempting to access the SSID:
  - Passphrase—When enabled, you must configure a passphrase (8-63 ASCII characters) that permits access to the SSID.
  - PSK—When enabled, you must enter a pre-shared key (256 bit/64 characters hexadecimal) that permits access to the SSID.

- Encryption—The encryption setting specifies the encryption method used between the security device and wireless clients in the subnetwork. Select one of the following:
  - AES—The American Encryption Standard (AES) is used by WPA 2 devices. AES uses the Robust Security Network (RSN) cipher for encryption. This complex encryption mechanism is a block cipher (operates on 128 bit data blocks).
  - TKIP—The temporal key integrity protocol (TKIP) is used by WPA 1 devices. TKIP is a key management protocol that handles key generation and key synchronization; TKIP uses the RC4 algorithm for encryption.
  - Auto—When enabled, the device uses the encryption method (AES or TKIP) used by the client.

### Reactivating Wireless Connections

When you make changes to the wireless settings on the security device, you must update the device with your changes before the new settings take effect.

**NOTE:** When using an authentication server for wireless authentication, if you enable 802.1X support on that server, you must also reactivate the WLAN subsystem before the change can take effect.

Additionally, the device must reactivate its WLAN subsystem to use the new settings. **NetScreen-Security Manager automatically reactivates the WLAN subsystem within the NetScreen-5GT Wireless security device during the device update process.**

The reactivation process takes several seconds (approximately 10 seconds) to complete. During reactivation of the WLAN subsystem, the device severs all wireless connections and clears all wireless sessions from the session table. Previously connected wireless clients must reconnect to reestablish their disrupted sessions.
Conducting a Site Survey

When setting up the NetScreen-5GT Wireless (ADSL) device as a wireless access point (WAP), you can scan the broadcast vicinity to see if there are any other WAPs broadcasting nearby. A site survey detects any WAPs emitting a beacon in its area and records the following details about each detected WAP:

- Service set identifier (SSID)
- MAC address
- Received signal strength indicator (RSSI) The RSSI numbers are in decibels (dBs) that indicate the signal-to-noise ratio (SNR). The SNR is the signal level divided by the noise level, which results in a value representing signal strength.
- Broadcast channel

In addition to performing an initial site survey, you might want to perform occasional surveys to ensure that no rogue WAPs are operating in the area.

A site survey takes about 5-10 seconds to complete.

Configuring the Network Module

Some security device systems, such as the NetScreen 500, NetScreen-5000 series and ISG series, contain physical slots in which you can install optional modules.

Viewing Slot Information

Use the Slot option on the device to view or set the type of network module installed in each available I/O slot in the physical device. Network modules include the following:

- Physical Interface Modules—the Secure Services Gateway (SSG) 520 and 550 security devices use wide area network (WAN) data links to transmit and receive traffic across geographically dispersed networks. You define the properties of the data link by configuring the WAN interface that corresponds to a port on an SSG Physical Interface Module (PIM).

- Copper and Fiber Interface Modules—these modules provide additional ethernet ports.

- Management Modules—these modules provide management functionality for the ISG 2000 and 1000 series devices. The NetScreen-5000 series network modules are known as Security Port Modules (SPMs); SPMs handle general packet processing at Gigabit speeds, enabled by ASIC support.

**NOTE:** On SSG 520 and 550 security devices only, slot 0 is reserved for the device motherboard. The Card Type is referred to as “4 Ethernet interfaces (10/100/1000) fixed”.
The Chassis screens provide additional information about network modules installed in the available chassis slots of an ISG 2000 or ISG 1000 security device. The information displayed in the Chassis screens, including the version and serial number of the card, is obtained from the card installed in the physical device and is read-only.

You must configure the network module before physical interfaces appear in the NetScreen-Security Manager UI (even for imported devices).

Physical Interface Module

The SSG 520 and 550 devices support PIMs for the following WAN interface types:

- Serial
- T1
- E1
- T3 (also known as DS3)

Serial

Serial PIMs on SSG devices have two serial ports per PIM, which support full-duplex, synchronous data transmission. These ports can transmit packets at speeds up to 8 Megabits per second (Mbps). You cannot use these serial ports to connect a console or modem.

T1

T1 PIMs on SSG devices contain two T1 ports with integrated Channel Service Unit/Data Service Unit (CSU/DSU). These ports provide physical connections to T1 or fractional T1 network media types.

E1

E1 PIMs on SSG devices have two E1 ports with integrated Channel Service Unit/Data Service Unit (CSU/DSU). These ports provide physical connections to E1 or fractional E1 network media types.

T3 (also known as DS3)

Digital Signal level 3 (DS3) PIMs on SSG devices contain one physical DS3 port with integrated Data Service Unit (DSU). This port provides physical connection to T3 network media types at a bit rate of 44.736 megabits per second (Mbps).

Interface Modules (Copper)

A single security device can support a 10/100 Base-T and GBIC card simultaneously; however, the cards are not hot-swappable.
**10/100**

The 10/100Mbps interface module is typically used to support a 10 Base-T or 100 Base-T LAN. The card can support 2, 4, or 8 copper interfaces, and uses RJ-45 connectors with twisted pair.

---

**NOTE:** The ISG 2000 supports a maximum port count of 28. When using 8-port 10/100 modules in each I/O slot, ports five through eight in slot 4 are automatically disabled. You cannot configure these ports for firewall or HA functionality.

---

**10/100/1000**

The tri-mode card, available for ISG security devices, is a 2 ethernet port 10/100/1000Mbps IO card. The card supports 2 copper interfaces, uses RJ-45 connectors and twisted pair, and contains the following IO port configurations:

- 10Mbps Full/Half Duplex
- 100Mbps Full/Half Duplex
- 1000Mbps Full Duplex
- Auto (auto-negotiate link speed/duplex)

---

**Interface Modules (Fiber)**

Fiber interface module provide connectivity for fiber-based, gigabit ethernet LANs.

- **GB**
  - 1 interface (mini-GBIC). This card supports 1 fiber interface and uses an optical cable with SX or LX connectors.
  - 2 interfaces (GBIC). This card supports 2 fiber interfaces and uses an optical cable with SX or LX connectors.
  - GB LX/SX (2 interfaces). This card supports 2 fiber interfaces and uses an optical cable with SX and LX connectors.

---

**Secure Port Modules (SPM)**

Secure Port Modules (SPMs) provide general packet processing and device connection tasks for the NetScreen-5000 series. These modules are based on either the GigaScreen-II or Jupiter-II ASIC.

SPMs handle packets as they enter and exit the system, providing packet parsing, classification, and flow-level processing. SPMs also provide encryption, decryption, Network Address Translation (NAT), and session lookup features. When packets require additional processing, the device forwards the packets to the management module.

NetScreen-Security Manager supports the following SPMs for the NetScreen-5000 series security devices:
5000-8G SPM—This SPM provides eight 1-Gigabit Ethernet mini-Gigabit Interface Converter (GBIC) ports using hot-swappable transceivers. The 5000-8G delivers up to 4 Gigabits-per-second (Gbps) of firewall and up to 2 Gbps of Virtual Private Network (VPN) capacity. This module is also capable of supporting a total of four aggregate interfaces. The 5000-8G provides port Link and Activity LEDs in addition to Power and Status LEDs.

The 5000-8G2 SPM—This SPM provides eight 1-Gigabit Ethernet mini-Gigabit Interface Converter (GBIC) ports using hot-swappable transceivers. The 5000-8G2 SPM delivers up to 8 Gigabits-per-second (Gbps) of firewall and up to 4 Gbps of Virtual Private Network (VPN) capacity. This module is also capable of supporting a total of four aggregate interfaces, with up to four ports for each aggregate interface. The 5000-8G2 SPM provides port Link and Activity LEDs in addition to Power and Status LEDs.

5000-2G24FE SPM—This SPM provides two 1-Gigabit Ethernet ports and 24 FE ports with up to 2 Gbps of firewall and up to 1 Gbps of VPN process capacity. This module is capable of supporting a total of six aggregate interfaces. This total consists of one aggregate interface for the two 1-Gigabit ports, and five aggregate interfaces for the 24 10/100 Ethernet ports. Only similar ports can be aggregated together. You cannot aggregate a Gigabit port to a 10/100 FE port. The 5000-2G24FE provides port Link and Activity LEDs, in addition to Power and Status LEDs. Mini-GBIC transceivers are hot-swappable.

5000-2XGE SPM—This SPM provides two 10-Gigabit Ethernet ports using hot-swappable 10-Gigabit Small Form Factor Pluggable Module for PHY transceiver. The 5000-2XGE SPM delivers up to 10 Gigabits-per-second (Gbps) of firewall and up to 5 Gbps of Virtual Private Network (VPN) capacity. This module provides port Link and Activity LEDs in addition to Power and Status LEDs.

Viewing Chassis Information

For ISG security devices, you can view read-only information about the modules installed in the chassis of the device.

By default, the chassis includes a management module.

For ISG security devices running ScreenOS 5.0.0-IDP1, the chassis also includes the IDP security module.

Configuring Virtual Routers

Use the Virtual Router screens to configure routing on security devices. Routing is the process of forwarding packets from one network to another toward a final destination, and a router is a point where one network meets another network. Security devices contain integrated routing functionality that enables them to effectively forward protected traffic to its destination.

To configure a virtual router, double-click the virtual router in the Virtual Router configuration screen (or, either select the virtual router and then click the Edit icon, or right-click the virtual router and select Edit). You can configure the following parameters for a virtual router:
About Routes

You can configure three types of routing on a security device:

- **Static**—Static routes are mappings of IP network addresses to next-hop destinations that you define on a layer 3 forwarding device, such as a router. These mappings do not change unless you alter them. For networks that have few connections to other networks or where inter-network connections are relatively unchanging, it is usually more efficient to define static routes than to set up dynamic routing. The device retains static routes until you explicitly remove them. However, you can override static routes with dynamic routing information if necessary.

- **Dynamic**—Dynamic routing involves routers exchanging information about the reachability of networks and subnetworks and adjusting routing tables by analyzing incoming routing update messages. These messages populate the network, directing routers to recalculate routes and change their routing tables accordingly.

- **Multicast**—Multicast protocols enable routers to forward traffic from one source to multiple receivers simultaneously.

All routes are contained within a virtual router, as detailed below.

About Virtual Routers

A security device can divide its routing component into two or more virtual routers. A virtual router supports static routing, dynamic routing protocols, and multicast protocols, which you can enable simultaneously in one virtual router. A security device can contain the following types of Virtual Routers (VRs):

- **Predefined Virtual Routers**—Each security device contains two predefined virtual routers:
trust-vr. By default, contains all predefined security zones and any user-defined zones.

untrust-vr. By default, does not contain any security zones.

You cannot delete the trust-vr or untrust-vr predefined virtual routers.

Custom Virtual Routers—On some security devices, you can create and configure additional custom virtual routers.

You can define multiple VRs, but trust-vr is the default VR. All predefined and custom security zones (and all interfaces bound to those security zones) are bound to the trust-vr virtual router. To bind a security zone to the untrust-vr or to a custom VR, you must first unbind all interfaces from the zone. For a vsys, you can select a virtual router to be the default router for the vsys.

Configuring Virtual Router General Properties

You can configure the following general properties for a virtual router:

- Virtual Router ID—A unique identifier used to communicate with other routing devices. The identifier can be in the form of a dotted decimal notation, like an IP address, or an integer value. If you do not configure a specific virtual router ID before enabling a dynamic routing protocol, the device automatically selects the highest IP address of the active interfaces in the VR for the router identifier.

- Maximum Number of Routes—The maximum number of routing table entries that can be allocated for a specific virtual router. The maximum number of route entries available depends upon the security device and the number of virtual routers configured on the device. Setting the maximum number of route entries in a VR helps prevent one virtual router from using up all the entries in the system.

- Maximum Equal Cost Routes Supported (ScreenOS 5.1 and Higher Only)—The maximum Equal Cost Multi-Path (ECMP) routes used by the virtual router. You might want to use ECMP when load balancing to enable the route lookup to select a different route each time the route is invoked. This setting controls how many ECMP routes the route lookup can use; you can configure one to four ECMP routes for each virtual router. For example, when this setting is three and the number of available ECMP routes is five, the route lookup uses only the first three ECMP entries in the routing table (in round robin fashion) for the virtual router.

- Route Lookup Preference (ScreenOS 5.1 and higher Only)—Configure the order in which route lookup occurs. By default, route lookup uses the following sequence: SIBR routes (preferred value 3), Source-Based routes (preferred value 2), Destination-Based routes (preferred value 1). To change this sequence, configure the values for each preference from 1 to 255; the higher the value, the more preferred the route.

- Shared VR—You can make the VR accessible from any virtual system (vsys) on the device. By default, only the untrust-vr is a shared VR that is accessible by any vsys. You can configure other root-level VRs to be sharable.
- **Route Exporting**—(For the trust-vr only) You can enable or disable automatic route exporting to the untrust-vr for interfaces configured in Route mode.

- **Consider Active Routes**—You can direct the virtual router to consider active routes on inactive interfaces for redistribution or export. By default, only active routes defined on active interfaces can be redistributed to other protocols or exported to other virtual routers.

- **SNMP Private Traps**—You can specify the use of SNMP private traps for managing virtual router objects, including objects in the dynamic routing MIB. This option is only available for the default root-level virtual router.

- **Ignore Overlapping Subnets**—You can direct the virtual router to ignore overlapping subnet addresses for interfaces in the virtual router. By default, you cannot configure overlapping subnet IP addresses on interfaces in the same virtual router.

- **Next Hop**—(For the trust-vr only) You can direct the virtual router to use the untrust-vr as the next hop for the default route.

For step-by-step instructions on configuring virtual router general properties, see the NetScreen-Security Manager Online Help.

### Configuring Access Lists

An access list is a sequential list of statements against which a route is compared. Each entry in the list specifies the IP address/netmask of a network prefix and the forwarding status (whether to permit or deny the route).

For example, an entry in an access list can permit routes for the 1.1.1.0/24 subnetwork, while another entry in the same access list can deny routes for the 2.2.2.0/24 subnetwork. If a route matches an entry in the access list, the specified forwarding status is applied. If the two entries are in an access list, a route to the host at 1.1.1.10 is permitted, while the route to the host at 2.2.2.10 is denied.

You can also use access lists to control the flow of multicast control traffic. You can create an access list to restrict the multicast groups that hosts can join or the sources from which multicast traffic is received. After you create an access list, you can include it in a multicast rule.

The sequence of entries in an access list is important. A route is first compared to the entry in the access list with the lowest sequence number and then to other entries in ascending sequence number until there is a match. If there is a match, all subsequent entries in the access list are ignored. Therefore, you should sequence the more specific entries before less specific entries. For example, place the entry that denies routes for the 1.1.1.1/30 subnetwork before the entry that permits routes for the 1.1.1.0/24 subnetwork.

For step-by-step instructions on configuring virtual router access lists, see the NetScreen-Security Manager Online Help.

**EXAMPLE:** CREATING AN ACCESS LIST ON A VIRTUAL ROUTER

In this example, you create an access list on the trust-vr:
1. In Device Manager, double-click a device icon to open the device configuration. In the device navigation tree, select Network > Virtual Routers.

2. Double-click the trust-vr virtual router. The General Properties screen appears.

3. In the virtual router navigation tree, select Access List, then click the Add icon in the main display area. The Access List Entries/New dialog box appears.

4. For Access List Number, enter 2. This number uniquely identifies the access list.

5. In the Access List Entries area, click the Add icon. The New Access List Entry dialog box appears. Configure the following:
   a. For Sequence Number, enter 10. This number positions this statement relative to other statements in the access list.
   b. For Action, select Permit.
   c. For Prefix, select Prefix to Filter and enter the IP address/netmask 1.1.1.1/24.
   d. Click OK to save the new access list.

6. Click OK to save your changes to the virtual router, then click OK again to save your changes to the device configuration.

Configuring Route Maps

A route map is a set of statements that the device applies in sequential order to a route. Each statement in the route map defines a condition that is compared to the route. A route is compared to each statement in a specified route map in order of increasing sequence number until there is a match, then the action specified by the statement is applied. If the route matches the condition in the route map statement, the route is either permitted or rejected.

A route map statement can also modify certain attributes of a matching route. There is an implicit deny at the end of every route map; that is, if a route does not match any entry in the route map, the route is rejected.

For each match condition, you specify whether a route that matches the condition is accepted (permitted) or rejected (denied). If a route matches a condition and is permitted, you can optionally set attribute values for the route. You can configure additional entries for the same route map, specifying a different sequence number for each entry.

Configuring Route Map Match Conditions

You can configure the following match conditions for a route map:

- AS Path (BGP)—Select the AS path Access List a route must match. For details, see “Configuring Access Lists” on page 173.

- Community (BGP)—Select the Community a route must match. For details, see “Configuring Access Lists” on page 173.
Metric—Select the route metric a route must match.

Interface—Select the interfaces a route must match.

Access List—Select the access list a route must match. For details, see “Configuring Access Lists” on page 173.

Next-Hop—Matches a specified Access List. For details, see “Configuring Access Lists” on page 173.

Route Type (OSPF)—Select the route types (OSPF internal, external type 1, or external type 2) that a route must match.

Tag—Select the route tag value a route must match.

Configuring Permitted Route Attributes
You can configure the following attributes for matching permitted routes:

- AS Path (BGP)—Prepends a specified AS path access list to the path list attribute of the matching route.
- Community (BGP)—Sets the community attribute of the matching route to the specified community list.
- Next-Hop—Sets the next-hop of the matching route to the specified IP address.
- Tag—Sets the tag of the matching route to the specified tag value or IP address.
- Weight—Sets the weight of the matching route.
- Metric Type (OSPF)—Sets the OSPF metric type of the matching route to either external type 1 or external type 2.
- Local Preference (BGP)—Sets the local-pref attribute of the matching route to the specified value.
- Preserve preference (ScreenOS 5.1 and higher Only)—Preserves the preference value of the matching route that is exported into another virtual router.
- Metric—Select one of the following to configure how the virtual router assigns a metric to permitted routes:
  - Use Metric Specified By User as Imported/Exported Route Metric. When enabled, the VR assigns the specified metric value to all matching routes.
  - Use the Source Route Metric as the Imported/Exported Route Metric. When enabled, the VR preserves the metric of a matching route that is imported or exported into another virtual router.
- **Offset Metric (ScreenOS 5.1 and higher Only)**—When enabled, the VR increments the metric of the matching route by the specified number. Use this option to increase the metric on a less desirable path. For RIP routes, you can apply the increment to either routes advertised (route-map out) or routes learned (route-map in). For other routes, you can apply the increment to routes that are exported into another virtual router.

For step-by-step instructions on configuring virtual router route maps, see the NetScreen-Security Manager Online Help.

### Configuring Export and Import Rules

When the security device has multiple virtual routers, you can enable one VR to learn specified routes in another VR.

- Use an **export rule** on the source VR to export specific routes to the destination VR. When exporting routes, a virtual router permits other VRs to learn about its network.

- Use an **import rule** on the destination VR to import specific routes from the source VR. Import rules control which routes can be imported; if the destination VR does not contain any import rules, the destination VR accepts all exported routes, however, if you create an import rule, the destination VR accepts only the routes specified in the import rule.

Configuring an export or import rule is similar to configuring a redistribution rule. You configure a route map to specify which routes are to be exported/imported and the attributes of the routes.

You can also configure the trust-vr to automatically export all its route table entries to the untrust-vr, or configure a user-defined virtual router to automatically export routes to other virtual routers. However, this does not necessarily mean that the untrust-vr imports all the routes exported by the trust-vr. If you define import rules for the untrust-vr, only routes that match the import rules are imported.

For step-by-step instructions on configuring virtual router export and import rules, see the NetScreen-Security Manager Online Help.

#### EXAMPLE: Configuring an Export Rule on a Virtual Router

In this example, you export OSPF routes for the 1.1.1.1/24 network in the trust-vr virtual router to the untrust-vr routing domain. You first create an access list for the network prefix 1.1.1.1/24, which is then used in the route map “rtmap1” to filter for matches of routes for the 1.1.1.1/24 network. You then create a route export rule to export matching OSPF routes from the trust-vr to the untrust-vr virtual router.

1. In Device Manager, double-click a device icon to open the device configuration. In the device navigation tree, select Network > Virtual Routers.

2. Double-click the trust-vr virtual router. The General Properties screen appears.

3. Configure the Access List:
   - In the virtual router navigation tree, select Access List, then click the Add icon in the main display area. The Access List Entries/New dialog box appears.
b. For Access List Number, enter 2.

c. In the Access List Entries area, click the Add icon. The New Access List Entry dialog box appears. Configure the following, then click OK:

- For Sequence Number, enter 10.
- For Action, select Permit.
- For Prefix, select Prefix to Filter and enter the IP address/netmask 1.1.1.1/24.

4. Configure the Route Map:

a. In the virtual router navigation tree, select Route Map, then click the Add icon in the main display area. The New Route Map dialog box appears.

b. For Name, enter rtmap1.

c. In the Route Map Entry area, click the Add icon. The New Route-Map Entry dialog box appears.

d. Configure as shown below:

Figure 37: Configure New Route Map for an Export Rule
For Sequence Number, enter 10.

For Action, select permit.

In the Match Properties area, in the Access List table, select 2.

e. Leave all other defaults and click OK to save the new route map entry.

5. Configure the Export Rule:

a. In the virtual router navigation tree, select Export Rules, then click the Add icon in the main display area. The New Export Rule dialog box appears.

b. Configure the following:

   - For Export to Virtual Router, select untrust-vr.
   - For Route Map, select rtmap1.
   - For Protocol, select OSPF.

c. Click OK to save the new export rule.

6. Click OK to save your changes to the virtual router, then click OK again to save your changes to the device configuration.

EXAMPLE: CONFIGURING AUTOMATIC EXPORT ON A VIRTUAL ROUTER

In this example, you configure the trust-vr to automatically export all routes to the untrust-vr. You also configure a route map on the untrust-vr to permit only internal OSPF routes.

1. In Device Manager, double-click a device icon to open the device configuration. In the device navigation tree, select Network > Virtual Routers.

2. Configure the export rule for the trust-vr:

   a. Double-click the trust-vr virtual router. The General Properties screen appears.

   b. In the main display area, select Auto-export route to untrust-vr.

   c. Click OK to save your changes to the trust-vr.

3. Configure the route map for the untrust-vr.

   a. Double-click the trust-vr virtual router. The General Properties screen appears.

   b. In the virtual router navigation tree, select Route Map, then click the Add icon in the main display area.

   c. For Name, enter from-ospf-trust.

   d. In the Route Map Entry area, click the Add icon. The New Route-Map Entry dialog box appears. Configure as shown below:
Figure 38: Configure New Route Map for an Auto-Export Route

### New Route Map

<table>
<thead>
<tr>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>from-ospf-trust</td>
</tr>
</tbody>
</table>

### Route Map Entry

<table>
<thead>
<tr>
<th>Sequence Number</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>Permit</td>
</tr>
</tbody>
</table>

### Match Properties

<table>
<thead>
<tr>
<th>AS Path</th>
<th>Community List</th>
<th>Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>none</td>
<td>none</td>
</tr>
</tbody>
</table>

### Interfaces

- ethernet1
- ethernet2
- ethernet3
- ethernet4
- ethernet5
- ethernet6
- ethernet7
- ethernet8

### Next Hop

- (empty)

### Route Type

- Internal OSPF
- Type 1 External OSPF
- Type 2 External OSPF

### Set Properties

<table>
<thead>
<tr>
<th>AS Path</th>
<th>Community List</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>none</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Next Hop</th>
<th>Tag</th>
<th>Offset Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>none</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Weight</th>
<th>Metric Type</th>
<th>Local Preference</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>none</td>
<td>none</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Metric</th>
<th>Use metric specified by user as imported/exported route metric.</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td></td>
</tr>
</tbody>
</table>
For Sequence Number, enter 10.

For Action, select permit.

In the Match Properties area, in the Route Type table, select Internal OSPF.

e. Click OK to save the new route map entry, then click OK again to save the route map.

4. Click OK to save your changes to the virtual router, then click OK again to save your changes to the device configuration.

Configuring Routing Table Entries

Typically, routers are attached to multiple networks and are responsible for directing traffic across these networks. Each router maintains a routing table, which is a list of known networks and directions on how to reach them. While processing an incoming packet on a security device, the router performs a routing table lookup to find the appropriate interface that leads to the destination address.

Each entry in a routing table—called a route entry or simply a route—is identified by the destination network to which traffic can be forwarded. The destination network, in the form of an IP address and netmask, can be an IP network, subnetwork, supernet, or a host. Routing table entries can originate from the following sources:

- Directly-connected networks (the destination network is the IP address that you assign to an interface in Route mode)
- Dynamic routing protocols, such as OSPF, BGP, or RIP
- Routes that are imported from other routers or virtual routers
- Statically-configured routes

You can configure three types of Static Routes: Destination-Based, Source-Based, and Source-Interface-Based routing. For each type of static route, you configure the following information:

NOTE: Source-interface-based routing is supported in ScreenOS 4.0.1-SIBR and ScreenOS 5.1 and higher.

- The interface on the security device on which traffic for the destination network is forwarded.
- The next-hop, which can be either another virtual router on the security device or a gateway IP address (usually a router address).
- The protocol from which the route is derived.
Preference (ScreenOS 5.1 and higher Only)—Controls the route to use when multiple routes to the same destination network exist. The lower the preference value of a route, the more likely the route is to be selected as the active route. By default, the preference value is automatically determined by the protocol or the origin of the route. You can modify a preference value from 1 to 255 for each protocol or route origin on a per-virtual router basis.

Metric (ScreenOS 5.1 and higher Only)—Controls the route used when multiple routes for the same destination network with the same preference value exist. The metric value for connected routes is always 0. The default metric value for static routes is 1, but you can specify a different value from 1 to 255 when defining a static route.

Keep route active when interface is down (ScreenOS 5.1 and higher Only)—Select this option to ensure that the route remains active even when the interface link status is down or the interface IP address is removed. By default, this option is disabled for all route entries. To enable this option for a Destination-Based route entry, you must configure the Next-Hop as a Gateway (not a Virtual Router).

The virtual system (vsys) to which this route belongs.

NOTE: In the routing table, you must configure a default route (network address 0.0.0.0/0) for the security device. You should also configure a route from the device to the IP address of the NetScreen-Security Manager Device Server.

For step-by-step instructions on configuring virtual router static route entries, see the NetScreen-Security Manager Online Help.

The following sections detail each static route type.

Configuring Destination-Based Routes

When a security device contains multiple virtual routers, the device does not automatically forward traffic between zones that reside in different VRs, even if the Security Policy permits that traffic. To enable traffic to pass from one virtual router to another, you can configure a static route in one virtual router that defines another VR as the next hop for the route. This route can even be the default route for the virtual router. For example, you can configure a default route for the trust-vr with the untrust-vr as the next hop. If the destination in an outbound packet does not match any other entries in the trust-vr routing table, it is forwarded to the untrust-vr.

To create a static route for a network destination, you must enter the IP address and netmask for the destination network, then select either Virtual Router or Gateway as the Next Hop:

- If the Next Hop is a Virtual Router, you must also select the VR that is to be the next hop for the route.
- If the Next Hop is a Gateway, you must also enter the interface through which the next hop router is accessed, the IP address of the next hop router, and the metric and tag for the route.
For devices running ScreenOS 5.2, you can also configure Gateway Tracking to manage the route. When enabled, Gateway Tracking deactivates a route when the gateway becomes unreachable. When the gateway become reachable again, Gateway Tracking reactivates the route. Gateway Tracking is supported only for destination-based route table entries.

For step-by-step instructions on configuring virtual router destination-based route entries, see the NetScreen-Security Manager Online Help.

**NOTE:** For security devices running ScreenOS 5.3, you can also configure source-based and source-interface-based routes with next hop as a virtual router within the same security device.

### Configuring Source-Based Routing

Some security devices also enable you to configure a route entry based on the source IP address of the data packet.

To create a static route for a network destination, you must enter the IP address and netmask for the destination network, then select the interface through which the next hop router is accessed. You must also enter the IP address of the next hop router and configure a metric for the route.

For step-by-step instructions on configuring virtual router source-based route entries, see the NetScreen-Security Manager Online Help.

**EXAMPLE: USING SOURCE-BASED ROUTING**

In the following example, you want to forward traffic from the 10.1.1.0/24 subnetwork to ISP 1, and forward traffic from the 10.1.2.0/24 subnetwork to ISP 2. You must configure two entries in the default trust-vr virtual router routing table and enable source-based routing. The subnetwork 10.1.1.0/24, with ethernet1 as the forwarding interface, uses the ISP 1 router (1.1.1.1) as the next-hop; subnetwork 10.1.2.0/24, with ethernet2 as the forwarding interface, uses the ISP 2 router (2.2.2.2) as the next-hop.

**Figure 39: Source-Based Routing Example Overview**

1. Double-click the device icon to open the device configuration. In the device navigation tree, select Network > Virtual Routers. Double-click the trust-vr virtual router. The General Properties screen appears.
2. In the router navigation tree, select Routing Table.

3. Select Enable Source-Based Routing.

4. Add the first routing entry:
   a. In the Source-Based Routing Table area, click the Add icon. The New Source Routing Table dialog box appears.
   b. Configure the following:
      - For IP Address, enter 10.1.1.0.
      - For Network Mask, enter 24.
      - For Interface, select ethernet1
      - For Gateway, enter the IP address 1.1.1.1
   c. Click OK to save the new routing entry.

5. Add the second routing entry:
   a. In the Source-Based Routing Table area, click the Add icon. The New Source Routing Table dialog box appears.
   b. Configure the following:
      - For IP Address, enter 10.1.2.0.
      - For Network Mask, enter 24.
      - For Interface, select ethernet2
      - For Gateway, enter the IP address 2.2.2.2
   c. Click OK to save the new routing entry.

6. Confirm that your routing table is similar to the one shown below:

   Figure 40: Confirm Entries for Source-Based Routing Table

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Network Mask</th>
<th>Interface</th>
<th>Gateway</th>
<th>Metric</th>
<th>Vsys</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.2.0</td>
<td>24</td>
<td>ethernet2</td>
<td>2.2.2.2</td>
<td>1</td>
<td>...</td>
</tr>
<tr>
<td>10.1.1.0</td>
<td>24</td>
<td>ethernet1</td>
<td>1.1.1.1</td>
<td>1</td>
<td>...</td>
</tr>
</tbody>
</table>

7. Click OK to save your changes to the device.
Configuring Source-Interface-Based Routing

Some security devices also enable you to configure a route entry based on the source interface (the interface on which a data packet arrives). You can use source-based-interface routing (SIBR) to enable traffic from users on a specific subnet to be forwarded on one path while traffic from users on a different subnet is forwarded on another path.

NOTE: Source-interface-based routing is supported in ScreenOS 4.0.1-SIBR and ScreenOS 5.1 and higher.

SIBR can be used in conjunction with the source-based routing feature, which enables traffic to be forwarded based on the source IP address of a data packet. When a security device performs route lookup, the source-interface-based routing table is checked first. If the route is not found in the source-interface-based routing table and if source-based routing is enabled, the source-based routing table is checked. If the route is not found in the source-based routing table, the destination-based routing table is checked.

You define source-interface-based routes as static routes on a specific virtual router and source interface. Source-interface-based routes only apply to the virtual router in which you configure them. For example, you cannot specify another virtual router as the next-hop for a source-interface-based route. You also cannot redistribute source-interface-based routes into another virtual router or into a routing protocol.

When configuring SIBR, you must specify the name of the interface in the virtual router on which the packet arrives, then set the interface on which the packet is to be forwarded. This interface can belong to a zone in another virtual router, if that virtual router is sharable. (Sharable virtual routers are VRs that are accessible by any vsys on the device. The untrust-vr is, by default, a sharable virtual router, but you can configure other root-level VRs to be sharable). Next, enter the IP address of the next hop router in Gateway. If you have already specified a default gateway for the interface, you do not need to specify this parameter; the interface’s default gateway is used for the source-interface-based route.

You can also configure a metric for the route, if desired. By default, the metric for all SIBR entries is 1. If there are multiple source-interface-based routes with the same prefix, only the route with the best (lowest) metric is used for route lookup and other routes with the same prefix are marked as “inactive”.

For step-by-step instructions on configuring virtual router source interface-based route entries, see the NetScreen-Security Manager Online Help.

EXAMPLE: CONFIGURING SOURCE INTERFACE-BASED ROUTING

In the following example, you want to forward traffic from the 10.1.1.0/24 subnetwork to ISP 1, and forward traffic from the 10.1.2.0/24 subnetwork to ISP 2. You must configure two entries in the default trust-vr virtual router routing table and enable source-based routing. The subnetwork 10.1.1.0/24, with ethernet2/1 as the source interface and ethernet2/3 as the forwarding interface, uses the ISP 1 router (1.1.1.1) as the next-hop; subnetwork 10.1.2.0/24, with ethernet2/2 as the source interface and ethernet2/4 as the forwarding interface, uses the ISP 2 router (2.2.2.2) as the next-hop.
1. Add a NetScreen-5400 device running ScreenOS 4.0.1SIBR, then configure the network module:
   a. Double-click the device icon to open the device configuration. In the device navigation tree, select Network > Slot.
   b. Double-click slot 2 to display the slot configuration dialog box. For Card Type, select 5000-8G SPM.
   c. Click OK to save the slot configuration, then click Apply to apply the new interfaces to the device.

2. Configure the ethernet 2/1 and ethernet 2/3 interfaces:
   a. In the device navigation tree, select Network > Interface.
   b. Double-click the ethernet2/1 interface. The General Properties screen appears. Configure as follows:
      ■ For Zone, select Trust.
      ■ For IP address and Netmask, enter 10.1.1.0/24.
   c. Click OK to save your changes to the interface.
   d. Double-click the ethernet2/3 interface. The General Properties screen appears. Configure as follows:
      ■ For Zone, select Trust.
      ■ For IP address and Netmask, enter 10.1.2.0/24.
   e. Click OK to save your changes to the interface.

3. In the device navigation tree, select Network > Virtual Routers. Double-click the trust-vr virtual router. The General Properties screen appears. In the router navigation tree, select Routing Table.

4. Select Enable Source-Based Routing.
5. Configure the first entry:
   a. In the Source-Interface-Based Routing Table area, click the Add icon.
   b. Configure the following:
      - For Incoming Interface, select ethernet2/1.
      - For IP Address and Netmask, enter 10.1.1.0/24
      - For Interface, enter ethernet2/3.
      - For Gateway IP Address, enter 1.1.1.1
   c. Click OK to save the SIBR entry.

6. Configure the second entry:
   a. In the Source-Interface-Based Routing Table area, click the Add icon.
   b. Configure the following:
      - For Incoming Interface, select ethernet2/3.
      - For IP Address and Netmask, enter 10.1.2.0/24
      - For Interface, enter ethernet2/4.
      - For Gateway IP Address, enter 2.2.2.2
   c. Click OK to save the SIBR entry.

7. Click OK to save your changes to the virtual router, then click OK to save your changes to the device.

Configuring Route Preferences

A route preference is a weight added to the route that influences the determination of the best path for traffic to reach its destination. When importing or adding a route to the routing table, the virtual router adds a preference value—determined by the protocol by which the route is learned—to the route. A low preference value (a number closer to 0) is preferable to a high preference value (a number further from 0). In a virtual router, you can set the preference value for routes according to protocol.

To change the preference value for a protocol, enter a new value for the protocol in the Route Preferences configuration screen.

Configuring Dynamic Routing

This section describes the basic steps in configuring the following dynamic routing protocols:

- Configuring Open Shortest Path First (OSPF)
Configuring Open Shortest Path First (OSPF)

The Open Shortest Path First (OSPF) routing protocol operates within a single Autonomous System (AS). A router running OSPF distributes its state information (such as usable interfaces and neighbor reachability) by periodically flooding link-state advertisements (LSAs) throughout the AS.

Each OSPF router uses LSAs from neighboring routers to maintain a link-state database, a listing of topology and state information for the surrounding networks. The constant distribution of LSAs throughout the routing domain enables all routers in an AS to maintain identical link-state databases. OSPF uses the link-state database to determine the best path to any network within the AS by generating a shortest-path tree (a graphical representation of the shortest path to any network within the AS). While all routers have the same link state database, they all have unique shortest-path trees because a router always generates the tree with itself at the top of the tree.

To enable OSPF on a security device, you must first enable OSPF on a virtual router, then enable OSPF on individual interfaces. You can also configure optional OSPF settings, such as the following:

- Global settings, such as virtual links, that are set at the VR level for the OSPF protocol.
- Interface settings, such as authentication, that are set on a per-interface basis for the OSPF protocol. When you configure an OSPF parameter at the interface level, the parameter setting affects the OSPF operation only on the specific interface.

Additionally, you can set security-related OSPF settings at either the VR level or on a per-interface basis. The following sections detail how to enable OSPF and configure all optional parameters.

Enabling OSPF

To enable OSPF on a security device, you must first create an OSPF instance on a virtual router, then enable OSPF on individual interfaces.

To create and OSPF instance in a virtual router:

1. In the device navigation tree, select Network > Virtual Router and double-click the virtual router for which you want to configure OSPF.

2. In the router navigation tree, select Dynamic Routing Protocol, then select Configured OSPF Instance. The OSPF settings appear in the router navigation tree.

3. Select OSPF > Parameters, then select Enable OSPF. If desired, configure additional global and security settings, as detailed in “Configuring Global OSPF Settings” on page 188.
4. Click OK to save your changes to the virtual router.

To enable OSPF on an interface:

1. In the device navigation tree, select Network > Interface and double-click the interface for which you want to configure OSPF.

2. In the interface navigation tree, select Protocol and select the OSPF tab.

3. Select Enable OSPF. If desired, configure additional interface and security settings, as detailed in “Configuring OSPF Interface Parameters” on page 190.

4. Click OK to save your changes to the interface.

Configuring Global OSPF Settings

A global OSPF setting affects operations on all OSPF-enabled interfaces. You configure global settings in the virtual router.

For step-by-step instructions on configuring OSPF settings on the virtual router and on the interface, see the NetScreen-Security Manager Online Help.

Configuring OSPF Parameters

You can configure the following parameters for an OSPF instance:

- Automatically Generate Virtual Links—Select this option to direct the VR to automatically create a virtual link for instances when it cannot reach the network backbone. By default, this option is disabled.

- Reject Default Route—Select this option to prevent Route Detour Attacks, in which a router injects a default route (0.0.0.0/0) into the routing domain in order to detour packets to itself. During a router detour, a compromised router can then either drop the packets, causing service disruption, or it can obtain sensitive information in the packets before forwarding them. By default, this option is disabled, meaning OSPF accepts any default routes that are learned in OSPF and adds the default route to the routing table.

- RFC 1583 Compatible—Select this option to make the OSPF routing instance compatible with RFC 1583, an earlier version of OSPF. By default, security devices support OSPF version 2, as defined by RFC 2328.

- Prevent Hello Packet Flooding Attack—Configure the Maximum Hello Packets threshold accepted by the VR. By default, the OSPF hello packet threshold is 10 packets per hello interval. You might want to use this setting to prevent a malfunctioning or compromised router from flooding its neighbors with OSPF hello packets.

- Prevent LSA Flooding Attack—Configure the number of LSAs accepted by the VR. By default, the VR accepts all LSAs. You might want to use this setting to prevent a malfunctioning or compromised router from flooding its neighbors with OSPF LSA packets. During an LSA flood attack, a router generates an excessive number of LSAs in a short period of time, thus keeping other OSPF routers in the network busy running the SPF algorithm.
Advertising Default Route—Select this option to direct the VR to advertise an active default route (0.0.0.0/0) in the VR route table to all OSPF areas.

Configuring OSPF Areas
By default, all routers are grouped into a single “backbone” area called area 0 (usually denoted as area 0.0.0.0). However, you might want to segment large geographically dispersed networks into multiple areas for better scalability.

Using multiple areas reduces the amount of routing information passed throughout the network because a router only maintains a link-state database for the area in which it resides. The VR maintains link-state information for all connected areas, and does not maintain link-state information for networks or routers outside the area.

AS external advertisements describe routes to destinations in other autonomous systems and are flooded throughout an AS. To prevent AS external advertisements from flooding an AS, configure the OSPF area as a stub area:

- **Stub area**—An area that receives route summaries from the backbone area but does not receive link-state advertisements from other areas for routes learned through non-OSPF sources (BGP, for example). A stub area can be considered a totally stubby area if no summary routes are allowed in the stub area.

- **Not So Stubby Area (NSSA)**—Like a normal stub area, NSSAs cannot receive routes from non-OSPF sources outside the current area. However, external routes learned within the area can be learned and passed to other areas.

All areas must connect to area 0, which is defined by default on the virtual router when you enable the OSPF routing instance on the virtual router. For areas that cannot be physically connected to the backbone area, you must configure a virtual link to provide the remote area with a logical path to the backbone through another area. For details on virtual links, see “Configuring OSPF Virtual Links” on page 190.

Configuring OSPF Summary Import
In large internetworks where hundreds or even thousands of network addresses can exist, routers can become overly congested with route information. After you have redistributed a series of routes from an external protocol to the current OSPF routing instance, you can bundle the routes into one generalized or summarized network route. By summarizing multiple addresses, you enable a series of routes to be recognized as one route, simplifying the process.

Using route summarization in a large, complex network can isolate topology changes from other routers. An intermittently failing link in a domain does not affect the summary route, so no router external to the domain needs to modify its routing table due to the link failure. Route summarization also prevents LSAs from propagating to other areas when a summarized network goes down or comes up.

You can summarize inter-area routes or external routes.
Configuring OSPF Redistribution Rules

Use route redistribution to exchange of route information between routing protocols. You can redistribute the following types of routes into the OSPF routing instance in the same VR:

- Routes learned from BGP
- Directly connected routes
- Imported routes
- Statically configured routes

When you configure route redistribution, you must first specify a route map to filter the routes that are redistributed.

Configuring OSPF Virtual Links

All areas must connect to area 0, which is the backbone. Area 0 is defined by default on the virtual router when you enable the OSPF routing instance on the virtual router. For areas that cannot be physically connected to the backbone area, you must configure a virtual link to provides the remote area with a logical path to the backbone through another area.

To enable a virtual link, the virtual link must exist on routers at both ends of the link. Specifically, you must configure:

- Area ID—The ID of the OSPF area through which the virtual link passes. You cannot create a virtual link that passes through the backbone area or a stub area.
- Router ID—The ID of the router at the other end of the virtual link.

Configuring OSPF Interface Parameters

By default, OSPF is disabled on all interfaces in the VR. You must enable OSPF on an interface before OSPF can use that interface to transmit receive packets. When you disable OSPF on an interface, OSPF does not transmit or receive packets on the specified interface, but interface configuration parameters are preserved.

For step-by-step instructions on configuring OSPF settings on the virtual router and on the interface, see the NetScreen-Security Manager Online Help.

You can enable OSPF on ethernet and tunnel interfaces. When configuring OSPF on a tunnel interface, you can configure additional parameters to keep OSPF tunnel traffic to a minimum.

You can configure the following OSPF interface parameters:

- Bind to Area—Select a previously-created area to bind the interface to that area. By default, all interfaces are bound to area 0, the backbone area.
Cost—Configure the metric for the interface. The cost associated with an interface depends upon the bandwidth of the link to which the interface is connected. The higher the bandwidth, the lower (more desirable) the cost value.

Hello Interval—Configure the number of seconds that the interface sends out OSPF hello packets to the network. By default, the interface sends 10 hello packets per second.

OSPF Priority—Configure the priority level of the VR elected by the interface. The router (Designated Router or Backup Designated Router) with the larger priority value has the best chance (although not guaranteed) chance of being elected.

Retransmit Interval—Configure the number of seconds that elapse before the interface resends an LSA to a neighbor that did not respond to the original LSA. By default, the interface resends an unacknowledged LSA every 5 seconds.

Transmit Delay—Configure the number of seconds between transmissions of link-state update packets sent on the interface. By default, the interface sends link-state updates every second.

Configuring Interface Link Type—Configure how the interface forms adjacencies with other routers:

- A Point-to-Point interface for OSPF forms an adjacency with only one OSPF router in the area. If the local tunnel interface is to be bound to multiple tunnels, you must configure the local tunnel interface as a point-to-multipoint interface.

- A Regular Multicast Interface for OSPF acts as a broadcast interface, and forms adjacencies with all routers in the area.

Enable Reduction in LSA Flooding (ScreenOS 5.1 and higher Only)—Select to suppress LSA packets. When this option is enabled, the device sends LSA packets only when the LSA content has changed. By default, this option is disabled.

Configure to Ignore MTU Mismatch in DB Exchange (ScreenOS 5.1 and higher Only)—Select to ignore any mismatches in maximum transmission unit (MTU) values between the local and remote interfaces that are found during OSPF database negotiations. Use this option only when the MTU on the local interface is lower than the MTU on the remote interface.

Interface OSPF Passive Mode—Select to prevent the interface from transmitting or receiving packets. The IP address of the interface is still advertised on the OSPF domain as an OSPF route and not as an external route. You might want to select this option when BGP is also enabled on the interface.

You can configure the following additional OSPF parameter for tunnel interfaces:
Configuring Demand Circuit (ScreenOS 5.1 and higher Tunnel Interfaces Only)—Configure the tunnel interface as an OSPF demand circuit (a network segment on which connect time or usage affects the cost of using such connection). When traversing a demand circuit, the security device limits routing protocol traffic to changes in network topology, and suppresses sending OSPF hello packets and periodic refreshment of LSA flooding. To configure an interface as a demand circuit:

- The Interface Link Type must be point-to-point or serial; you cannot configure a point-to-multipoint interface as a demand circuit.
- You must configure both ends of the tunnel as demand circuits.

Configuring OSPF Neighbors

Two routers with interfaces on the same subnet are considered neighbors. Routers use the hello protocol to establish and maintain these neighbor relationships. When two routers establish bidirectional communication, they are said to have established an adjacency. If two routers do not establish an adjacency, they cannot exchange routing information. By default, the OSPF routing instance on the virtual router forms adjacencies with all OSPF neighbors communicating on an OSPF-enabled interface.

You can configure the following settings for Neighbors on the interface:

- Neighbor Dead Interface—Enter the number of seconds that elapses with no response from an OSPF neighbor before OSPF determines the neighbor is not running. By default, OSPF determines a neighbor is “dead” after 40 seconds.
- Add/Edit/Delete Neighbor (Ethernet Interface Only)—To limit the devices on an interface that can form adjacencies with the OSPF routing instance, define the subnets that contain eligible OSPF neighbors. Only hosts or routers that reside in the specified subnets can form adjacencies with the OSPF routing instance.

NOTE: All OSPF routers in an area must use the same hello, dead, and retransmit interval values before they can form adjacencies.

Configuring OSPF Authentication

Because LSAs are unencrypted, most protocol analyzers can decapsulate OSPF packets. Authenticating OSPF neighbors using MD5 authentication or simple password is the best way to fend off these types of attacks.

When authentication is enabled, the device discards all unauthenticated OSPF packets received on the interface. By default, authentication is disabled.

To enable authentication, select one of the following authentication methods:

- Clear Text Authentication—To use a simple password for authentication, select this option and enter the password.

NOTE: All passwords handled by NetScreen-Security Manager are case-sensitive.
Multiple MD5 Authentication— To use MD5 keys for authentication, select this option, then configure the active MD5 key.

- To use an existing MD5 key, select the key ID as the Active MD5 Key ID.
- To add a new MD5 key, click the Add icon and configure a Key ID for the new MD5 key.

**NOTE:** You must use the same MD5 key for the sending and receiving OSPF routers.

**EXAMPLE: CONFIGURING OSPF**

To configure OSPF:

1. In the navigation tree, select Device Manager > Security Devices. Double-click the device object to open the device configuration.

2. In the device navigation tree, select Network > Virtual Router to display the list of configured virtual routers. Double-click the virtual router in which you are configuring an OSPF routing instance. The Virtual Router configuration screen appears.


4. In the virtual router navigation tree, select OSPF > Parameters to display the Parameters screen. Select OSPF, then click OK to close the Parameters screen.

5. To define a new non-backbone OSPF area, select OSPF > Area. The Area configuration screen appears. In this screen, do the following:
   a. Click the Add icon.
   b. Enter the Area ID.
   c. Select the interfaces that are to be included in this OSPF area.
   d. Select the Type.
   e. Click OK to close the Area configuration screen.

6. In the device navigation tree, select Interface to display the list of interfaces. Double-click the interface that is connected to OSPF peers to open the interface screen.

7. In the interface navigation tree, select Protocol to display the Protocol screen, then click the OSPF tab and configure the following:
   a. Select the ID of the OSPF area to which the interface is bound.
   b. Select OSPF.

8. Click OK.
Configuring Routing Information Protocol (RIP)

Routing Information Protocol (RIP) is a distance vector protocol used in moderate-sized autonomous systems (AS). Security devices support RIPv1 and RIPv2 (as defined by RFC 2453) and additional MD5 authentication extensions (as defined by RFC 2082).

Use RIP for dynamic routing on moderate-sized networks and to manage route information within a small, homogeneous, network such as a corporate LAN. The longest path allowed in a RIP network is 15 hops; a metric value of 16 indicates an invalid or unreachable destination. RIP supports both point-to-point networks (used with VPNs) and broadcast/multicast Ethernet networks. RIP does not support point-to-multipoint interfaces.

RIP maintains its own database of routes, including RIP protocol routes and redistributed routes. This database contains one entry for every destination that is reachable through the RIP routing instance. RIP adds the best routes to the VR routing table based on the virtual router’s ECMP limit (configured in the General Properties area of the virtual router) and the Alternate Route limit (configured in the virtual router’s RIP parameters). RIP sends out messages that contain the complete routing table to every neighboring router every 30 seconds. These messages are normally sent as multicasts to address 224.0.0.9 from the RIP port.

To enable RIP on a security device, you must first enable RIP on a virtual router, then enable RIP on individual interfaces. You can also configure optional RIP settings, such as the following:

- Global settings, such as timers and trusted RIP neighbors, that are set at the VR level for the RIP protocol.

- Interface settings, such as authentication, that are set on a per-interface basis for the RIP protocol. When you configure a RIP parameter at the interface level, the parameter setting affects the RIP operation only on the specific interface.

Additionally, you can set security-related RIP settings at either the VR level or on a per-interface basis. The following sections detail how to enable RIP and configure all optional parameters.

Enabling RIP

To enable RIP on a security device, you must first create a RIP instance on a virtual router, then enable RIP on individual interfaces.

To create a RIP instance on a virtual router:

1. In the device navigation tree, select Network > Virtual Router and double-click the virtual router for which you want to configure RIP.

2. In the router navigation tree, select Dynamic Routing Protocol and enable Configured RIP Instance. The RIP settings appear in the router navigation tree.

3. Select RIP > Parameters, then select Enable RIP. If desired, configure additional global and security settings, as detailed in “Configuring Global RIP Settings” on page 195.
4. Click OK to save your changes to the virtual router.

To enable RIP on an interface:

1. In the device navigation tree, select Network > Interface and double-click the interface for which you want to configure RIP.

2. In the interface navigation tree, select Protocol and select the RIP tab.

3. Select Enable RIP. If desired, configure additional interface and security settings, as detailed in “Configuring RIP Interface Parameters” on page 197.

4. Click OK to save your changes to the interface.

Configuring Global RIP Settings
A global RIP setting affects operations on all RIP-enabled interfaces. You configure global settings in the virtual router.

For step-by-step instructions on configuring RIP settings on the virtual router and on the interface, see the NetScreen-Security Manager Online Help.

Configuring RIP Parameters
You can configure the following parameters for an RIP instance:

- **RIP Version (ScreenOS 5.1 and higher Only)**—Select the version of RIP you want to use for this virtual router. When you configure RIP on the individual interfaces, you can override this setting.

- **Reject Default Route**—Select this option to prevent Route Detour Attacks, in which a router injects a default route (0.0.0.0/0) into the routing domain to detour packets to itself. During a route detour attack, a compromised router can drop the packets, causing service disruption, or can obtain sensitive information in the packets before forwarding them. By default, this option is disabled, meaning RIP accepts any default routes that are learned in RIP and adds the default route to the routing table.

- **Ignore Same Subnet Checking**—Select this option to allow RIP neighbors on different subnets.

- **Advertising Default Route**—Select this option to direct the VR to advertise an active default route (0.0.0.0/0) in the VR route table to all RIP areas.

- **Default Metric**—Configure the default metric for routes that RIP imports from other protocols, such as OSPF and BGP. By default, RIP assigns a metric of 10 to all imported routes.

- **Number of Alternate Routes for Prefix Allowed (ScreenOS 5.1 and higher Only)**—Configure the maximum number of RIP routes for the same prefix that RIP can add to the RIP route database. By default, RIP does not allow alternate routes.
Hold Down Time for Routes (ScreenOS 5.1 and higher Only)—Configure the number of seconds that RIP waits before updating the routing table. Use this option to prevent route flapping when handling high metric routes. By default, RIP waits 120 seconds between routing table updates. When configuring this option:

- Ensure that the value is at least three times the value of the Update Timer.
- Ensure that the value does not exceed the sum of the Update Timer value plus the Flush Timer value.

For example, if the Update Timer is 60 and the Flush Timer is 180, you can set the hold down time value between 181 and 239.

Retransmit Interval for Demand Circuits (ScreenOS 5.1 and higher Only)—Configure the number of seconds that elapse before RIP resends the RIP routing table to a demand circuit neighbor that did not respond. You can also configure the number of times RIP attempts to retransmit the routing table. By default, RIP resends every 5 seconds.

Poll Interval for Demand Circuits (ScreenOS 5.1 and higher Only)—Configure the number of seconds between demand circuit checks. By default, RIP sends a request through the demand circuit every three minutes to verify that the tunnel interface is up. You can also configure the number of times a demand circuit must fail to respond before RIP considers the circuit down. By default, RIP never considers an unresponsive circuit down (Number of Retries is 0).

Timers—Configure the following timers:

- Update Timer. Configure the number of seconds that the virtual router sends RIP route database updates to neighbors.
- Invalid Timer. Configure the number of seconds after a neighbor stops advertising a route that RIP considers the route invalid. By default, RIP considers a route invalid 180 seconds after a neighbor stops advertising it.
- Flush Timer. Configure the number of seconds an invalid route remains in the RIP route database. By default, RIP removes a route that has been invalid for 120 seconds.

Maximum Route Update Packets—Configure the maximum number of packets that the VR can receive per RIP update.

Maximum Neighbors Allowed on One Interface—Configure the maximum number of RIP neighbors allowed on a single interface. By default, RIP allows up to 16 neighbors for the same interface.

Access List for Filtering Trusted Neighbors—Configure the Access List that defines trusted RIP neighbors. If you do not select an access list, RIP uses multicasting or broadcasting to detect neighbors on a RIP-enabled interface.

Route Maps—To control which routes RIP learns and advertises, configure the following:

- The Inbound Route Map defines the routes that RIP learns.
The Outbound Route Map defined the routes that RIP advertises.

**Configuring RIP Redistribution Rules**

Use route redistribution to exchange of route information between routing protocols. You can redistribute the following types of routes into the RIP routing instance in the same VR:

- Routes learned from BGP
- Routes learned from OSPF
- Directly connected routes
- Imported routes
- Statically configured routes

When you configure route redistribution, you must first specify a route map to filter the routes that are redistributed.

**Configuring RIP Summary Import (ScreenOS 5.1 and higher Only)**

In large internetworks where hundreds or even thousands of network addresses can exist, routers can become overly congested with route information. After you have redistributed a series of routes from an external protocol to the current RIP routing instance, you can bundle the routes into one generalized or summarized network route. By summarizing multiple addresses, you enable a series of routes to be recognized as one route, simplifying the process.

Using route summarization in a large, complex network can isolate topology changes from other routers. An intermittently failing link in a domain does not affect the summary route, so no router external to the domain needs to modify its routing table due to the link failure.

You can summarize inter-area routes or external routes.

**Configuring RIP Interface Parameters**

By default, RIP is disabled on all interfaces in the VR. You must enable RIP on an interface before RIP can use that interface to transmit receive packets. When you disable RIP on an interface, RIP does not transmit or receive packets on the specified interface, but interface configuration parameters are preserved.

For step-by-step instructions on configuring RIP settings on the virtual router and on the interface, see the NetScreen-Security Manager Online Help.

You can enable RIP on ethernet and tunnel interfaces. When configuring RIP on a tunnel interface, you can configure additional parameters to keep RIP tunnel traffic to a minimum.

You can configure the following RIP interface parameters:

- Bind Interface to RIP—Select to bind this interface to RIP.
- Run Demand Circuit (ScreenOS 5.1 and higher Tunnel Interface Only)—Configure the tunnel interface as a RIP demand circuit (a network segment on which connect time or usage affects the cost of using such connection). When traversing a demand circuit, the security device limits routing protocol traffic to changes in network topology, and suppresses sending RIP packets. To complete the demand circuit, you must configure both ends of the tunnel as demand circuits.

- Enable Summarization (ScreenOS 5.1 and higher Only)—Select to enable route summarization on this interface. By default, the interface does not allow route summarization.

- Add/Edit/Delete RIP Neighbor (ScreenOS 5.1 and higher Only)—You can define the static RIP neighbors for the interface.

- RIP Versions (ScreenOS 5.1 and higher Only)—Select the version of RIP you want this interface to use for sending and receiving RIP information. By default, the interface uses the RIP version configured for the virtual router (Vrouter RIP Instance Version); if you select a different version, it overrides the virtual router setting.

- Metric—Configure the metric used for RIP routes from this interface.

- Passive Mode—Select to prevent the interface from transmitting packets (the interface can still receive packets). RIP advertises the IP address of the interface as a RIP route and not as an external route. By default, passive mode is disabled; however, you might want to select this option when BGP is also enabled on the interface.

- Route Maps—To control which routes RIP learns and advertises, select a previously-created Route Map for each of the following:
  - The Incoming Route Map Filter defines the routes that RIP learns.
  - The Outgoing Route Map Filter defines the routes that RIP advertises.

  These settings override the route maps configured on the virtual router.

- Split Horizon—Select Split-Horizon to prevent the interface from advertising learned routes in RIP updates sent to the same interface. When enabled, you can also select the Poison Reverse option, which instructs the interface to advertise learned routes with a metric of 16 when sending updates to the same interface. By default, split horizon is disabled.

**Configuring RIP Authentication**

Because RIP packets are unencrypted, most protocol analyzers can decapsulate them. Authenticating RIP neighbors using MD5 authentication or simple password is the best way to fend off these types of attacks. When authentication is enabled, the device discards all unauthenticated RIP packets received on the interface. By default, authentication is disabled.

To enable authentication, select one of the following authentication methods:
Clear Text Authentication—To use a simple password for authentication, select this option and enter the password.

NOTE: All passwords handled by NetScreen-Security Manager are case-sensitive.

Multiple MD5 Authentication—To use MD5 keys for authentication, select this option, then configure the active MD5 key.

- To use an existing MD5 key, select the key ID as the Active MD5 Key ID.
- To add a new MD5 key, click the Add icon and configure a Key ID for the new MD5 key.

NOTE: You must use the same MD5 key for the sending and receiving RIP routers.

Configuring Border Gateway Protocol (BGP)

Border Gateway Protocol (BGP) is a path-vector protocol that is used to carry routing information between autonomous systems (ASs). To configure BGP, you must create and enable the BGP routing instance in a virtual router by assigning an autonomous system number to the BGP instance, then enabling the instance. After you enable and configure the BGP peer, you can then enable BGP on the interface that is connected to the peer.

Before two BGP devices can communicate and exchange routes, they need to identify each other so they can start a BGP session. You need to specify the IP addresses of the BGP peers and, optionally, configure parameters for establishing and maintaining the session. Peers can be either internal (IBGP) or external (EBGP) peers. For an EBGP peer, you need to specify the autonomous system in which the peer resides.

All BGP sessions are authenticated by checking the BGP peer identifier and the AS number advertised by the peers. A successful connection with a peer is logged. If anything goes wrong with the peer connection, a BGP notification message is sent to or received from the peer, which causes the connection to fail or close.

For step-by-step instructions on configuring BGP settings on the virtual router and on the interface, see the NetScreen-Security Manager Online Help.

Route-Refresh Capability

NetScreen-Security Manager supports BGP route-refresh. This feature provides a soft reset mechanism that allows the dynamic exchange of route refresh requests and routing information between BGP peers and the subsequent re-advertisement of the outbound or inbound routing table.

Routing policies for a BGP peer using route-maps might impact inbound or outbound routing table updates because whenever a route policy change occurs, the new policy takes effect only after the BGP session is reset. A BGP session can be cleared through a hard or soft reset.
A soft reset allows the application of a new or changed policy without clearing an active BGP session. The route-refresh feature allows a soft reset to occur on a per-neighbor basis and does not require preconfiguration or extra memory.

A dynamic inbound soft reset is used to generate inbound updates from a neighbor. An outbound soft reset is used to send a new set of updates to a neighbor. Outbound resets don’t require preconfiguration or routing table update storage.

The route refresh feature requires that both BGP peers advertise route-refresh feature support in the OPEN message. If the route-refresh method is successfully negotiated, either BGP peer can use the route-refresh feature to request full routing information from the other end.

For more detailed information about zones on security devices, see the “Routing” volume in the NetScreen Concepts & Examples ScreenOS Reference Guide.

Configuring BGP Networks

Use the BGP Network settings to change the route attributes generated by BGP. For each route you want to change, create a new Network entry that contains the IP address and netmask for the network reachable from the BGP routing instance. Next, configure the new route attributes for that network:

- **Check Route Availability**—Configure how BGP determines route availability for this route:
  - Turn Off Reachability Check. When enabled, the BGP routing instance does not test whether it can reach the specified network.
  - Check for Same Route. When enabled, the BGP routing instance checks the prefix entered after the network for reachability; if reachable, the BGP routing instance adds the network.
  - Check Route Reachability. Select to direct the BGP routing instance to perform a test to determine whether it can reach the network you identified.

- **Configure Route Attributes (ScreenOS 5.1 and higher Only)**—Configure how BGP determines the route attributes for the specified route:
  - Weight. Select weight to assign a local preference value to the route that is not advertised to peers. If BGP uses more than one route to a destination, the route with the highest weight value is preferred.
  - Route Map. Select a previously-created route map to apply attributes for this route. BGP advertises the route with the route attributes specified in the selected route map.
Configuring Aggregate Addresses

As the number of BGP router addresses grows, each route in the AS requires more memory and CPU time to process addresses from the routing table. Using aggregation, BGP can reduce the size of a routing table by summarizing a range of addresses into a single route entry. Each address range included in the aggregate address is considered a contributing route within the aggregate address.

For each aggregate address you want to use, create a new Aggregate Address entry that contains the aggregate address IP and netmask. Next, configure the route attributes for the address:

- **AS Set**—When enabled, BGP generates AS set-path information for all contributing routes along with the aggregated route.
- **Summary Only**—When enabled, BGP advertises the aggregate route in place of the individual addresses for more specific contributing routes. If you select this option, you cannot configure a Suppress Route Map entry for this aggregate route.
- **Route Maps (ScreenOS 5.1 and higher Only)**—Configure a previously-created route map for each of the following:
  - **Advertise Route Map**—Select the previously-created route map that defines the path attributes for the aggregate route.
  - **Attribute Route Map**—Select the previously-created route map that defines the route attributes for the aggregate route.
  - **Suppress Route Map**—Select the previously-created route map that you want BGP to suppress for the aggregate route. If you select this option, you cannot enable Summary Only for this aggregate route.

Configuring Neighbors and Peer Groups

Use the Neighbor settings to configure individual peer addresses, called neighbors. You can also assign neighbors to a peer-group to configure parameters for the peer-group as a whole (you cannot assign IBGP and EBGP peers to the same peer-group).

Configuring a BGP Routing Instance

To configure BGP:

1. In the navigation tree, select Device Manager > Security Devices. Double-click the device object to open the device configuration.

2. In the device navigation tree, select Network > Virtual Router to display the list of configured virtual routers. Double-click the virtual router in which you are configuring a BGP routing instance. The Virtual Router configuration screen appears.

4. In the virtual router navigation tree, select BGP > Parameters to display the Parameters screen. Configure the following:

- Select BGP.
- Enter an AS Number.

5. In the virtual router navigation tree, select BGP > Neighbors to display the Neighbors screen. Click the Add icon to display the New Neighbor screen. Configure the following:

a. Select Peer Enabled.

b. Enter the BGP peer information.

c. Click OK to save the new neighbor.

d. Click OK to save your changes to the virtual router.

6. In the device navigation tree, select Interface to display the list of interfaces. Double-click the interface that is connected to the BGP peer to open the interface screen.

7. In the interface navigation tree, select Protocol to display the Protocol screen, then click the BGP tab and enable BGP.

8. Click OK.

### Configuring Multicast Routing

Multicast routing environments require the following to forward multicast information:

- A mechanism between hosts and routers to communicate group membership information. Security devices support the Internet Group Management Protocol (IGMP) versions 1, 2, and 3.

- A multicast routing protocol to populate the multicast route table and forward multicast traffic to hosts throughout the network. Security devices support the Protocol Independent Multicast-Sparse-Mode (PIM-SM) protocol. Alternatively, you can use IGMP Proxy to transmit multicast information between routers without the CPU overhead of a multicast routing protocol.

**NOTE:** Multicast routing is only supported in ScreenOS 4.0.1-Multicast and ScreenOS 5.1 and higher.

This section describes the basic steps to configure the following multicast protocols:

- Configuring IGMP
- Configuring IGMP Proxy
Configuring PIM-SM

NOTE: The NetScreen-Security Manager UI displays the multicast parameters and multicast static routes that you configure. It does not display dynamic information about multicast protocols at the device level. (For example, whether or not an interface is a Querier in IGMP.) For this information, you must issue the appropriate CLI "get" commands from the device.

Configuring IGMP

On security devices, you must explicitly enable IGMP in router mode on the interfaces that are connected to hosts. Security devices support the following Internet Group Management Protocol (IGMP) versions:

- IGMPv1, as defined in RFC 1112, Host Extensions for IP Multicasting, defines the basic operations for multicast group memberships.
- IGMPv2, as defined in RFC 2236, Internet Group Management Protocol, Version 2, expands on the functionality of IGMPv1.
- IGMPv3, as defined in RFC 3376, Internet Group Management Protocol, Version 3, adds support for source filtering. Hosts running IGMPv3 indicate which multicast groups they want to join and the sources from which they expect to receive multicast traffic. IGMPv3 is required when you run Protocol Independent Multicast in Source-Specific Multicast (PIM-SSM) mode.

To enable IGMP in router mode:

1. In the device navigation tree, select Network > Interface.
2. Double-click the interface on which you are enabling IGMP. The General Properties screen appears.
3. In the interface navigation tree, select Protocol.
4. Select the IGMP tab and configure the following:
   a. In the Type box, select Router.
   b. Select Enable.
5. Click OK to save your changes to the interface.
6. Click OK to save your changes to the device.

You can optionally change the default parameters for each interface on which IGMP is enabled. You can also use access lists to control traffic to and from an IGMP interface. First, create access lists that identify the following:

- The multicast groups that the hosts on a specified interface can join
- The hosts from which an IGMP router interface can receive IGMP messages
- The routers that are eligible for Querier selection
Then, enter the access list IDs in the IGMP configuration screen of the IGMP interface(s). The security device then filters IGMP traffic based on the access lists.

**Configuring IGMP Proxy**

IGMP proxy enables a security device to extend the scope of a multicast domain by one hop without running a multicast routing protocol. When you enable IGMP proxy on a device, the interface connected to the hosts (downstream interface) functions as a multicast router, and the interface connected to the upstream router functions as an IGMP host. You must first enable IGMP in host mode on upstream interfaces, then enable IGMP in router mode on downstream interfaces, and finally enable IGMP proxy on router interfaces.

To configure an IGMP proxy in the NetScreen-Security Manager UI:

1. In the device navigation tree, select Network > Interface.
2. Double-click the interface on which you are enabling IGMP. The General Properties screen appears.
3. In the interface navigation tree, select Protocol.
4. Select the IGMP.
   - If you are enabling IGMP on an upstream interface:
     - In the Type box, select Host.
     - Select Enable.
   - If you are enabling IGMP on a downstream interface:
     - In the Type box, select Router.
     - Select Enable.
     - Select Proxy.
5. Click OK to save your changes to the routing entry.
6. Click OK to save your changes to the device.

After you configure the interfaces, configure a multicast rule to permit IGMP messages to pass between zones. For information on multicast rules, see “Configuring Multicast Rules” on page 556.

**Configuring PIM-SM**

To configure PIM-SM in a virtual router on a security device:

1. Configure either a static route or a dynamic routing protocol such as RIP, BGP or OSPF. (For details on configuring static routes, see “Configuring Routing Table Entries” on page 180. For details on the dynamic routing protocols, see “Configuring Dynamic Routing” on page 186.)
2. Create a Security Policy to pass unicast and multicast data traffic between zones. (For details on Security Policies, see Chapter 9, “Configuring Security Policies”.)

3. Create and enable the PIM-SM routing instance in a virtual router.

4. Select PIM-SM on interfaces that transmit multicast traffic.

5. Configure a multicast rule to permit PIM-SM messages between zones. (For details on multicast rules, see “Configuring Multicast Rules” on page 556.)

After you enable the PIM-SM routing instance in the virtual router and enable it on all applicable interfaces, you can optionally configure PIM-SM features such as the following:

- Use access lists to restrict the rendezvous points (RPs) and sources from which a multicast group can receive traffic. You can also use access lists to restrict the multicast groups for which the virtual router forwards PIM join-prune messages. First, create the access lists, then enter the access list IDs in the PIM-SM configuration screen of the virtual router. The security device then uses the access lists to filter the PIM-SM traffic.

- Change the default parameters for each interface on which PIM-SM is enabled. When you set parameters at this level, the parameters affect the specific interface only.

- Configure a static RP for a particular zone, or use dynamic RP mappings and configure a virtual router as a candidate rendezvous point (C-RP).

- You can configure a virtual router to function as a proxy RP.

The following are the basic steps to configure PIM-SM in the NetScreen-Security Manager UI:

1. In the navigation tree, select Device Manager > Security Devices. Double-click the device icon to open the device configuration.

2. Configure the virtual router for PIM-SM:
   a. In the device navigation tree, select Network > Virtual Router.
   b. Double-click the virtual router in which you are configuring a PIM-SM instance. The General Properties screen appears.
   c. In the virtual router navigation tree, select Dynamic Routing Protocol.
   d. In the main display area, select Configure PIM-SM. PIM-SM configuration options now appear in the virtual router navigation tree under Dynamic Routing Protocol.
   e. In the virtual router navigation tree, select Dynamic Routing Protocol > PIM-SM > Parameters. The Parameters configuration screen appears.
   f. Select Enable in the main display area,
g. Click OK to save your changes to the virtual router.

3. Configure the interface for PIM-SM:
   a. In the device navigation tree, select Network > Interface.
   b. Double-click the interface that transmits multicast traffic. The General Properties screen appears.
   c. In the interface navigation tree, select Protocol, then select the PIM-SM tab in the main display area.
   d. Select Configure PIM-SM on Interface.
   e. Select Enable PIM-SM.
   f. Click OK to save your changes to the interface. Repeat step 3 to enable PIM-SM on additional interfaces.

4. Click OK to save your changes to the device configuration.

Configuring RP to Group Mappings

You can configure a static rendezvous point (RP) for a particular zone and/or configure a virtual router as a C-RP. Before you configure a static RP and a C-RP, you must first create access lists that identify the multicast groups mapped to each one.

Following are the basic steps for configuring an RP:

1. In the navigation tree, select Device Manager > Security Devices. Double-click the device icon to open the device configuration.

2. Configure the virtual router for PIM-SM:
   a. In the device navigation tree, select Network > Virtual Router.
   b. Double-click the virtual router in which you are configuring a PIM-SM instance. The General Properties screen appears.
   c. In the virtual router navigation tree, select Dynamic Routing Protocol.
   d. In the main display area, select Configure PIM-SM. PIM-SM configuration options now appear in the virtual router navigation tree under Dynamic Routing Protocol.

3. In the virtual router navigation tree, select Dynamic Routing Protocol > PIM-SM > Rendezvous Points.

4. In the main display area, click the Add icon. The new Zone dialog box appears. For Zone, select the zone that contains the RP.

5. To configure an Rendezvous Point Candidate:
   a. Select the interface that is advertised as the C-RP.
b. Specify the access list that identifies the multicast group(s) for which the interface is the RP candidate.

c. Select the advertised C-RP priority.

d. Select the holdtime advertised to the bootstrap router.

6. To configure a Static Rendezvous Point, click the Add icon in the Static RP Addresses area. The Static RP Addresses dialog box appears. Configure as follows:

   a. Enter the IP address of the RP.

   b. Specify the access list that identifies the multicast group(s) mapped to the RP.

   c. If you want to always use the same RP for the specified multicast group(s) select the Always used as RP check box. Use this option to override dynamic group-RP mappings.

7. Click OK to save your changes to the virtual router, then click OK to save your changes to the device configuration.

Configuring Acceptable Groups

You can create access lists to identify the acceptable sources, multicast groups and RPs, then configure the virtual router to accept PIM messages only from those specified in the access lists. To configure acceptable groups on the virtual router:

1. In the navigation tree, select Device Manager > Security Devices. Double-click the device icon to open the device configuration.

2. Configure the virtual router for PIM-SM:

   a. In the device navigation tree, select Network > Virtual Router.

   b. Double-click the virtual router in which you are configuring a PIM-SM instance. The General Properties screen appears.

   c. In the virtual router navigation tree, select Dynamic Routing Protocol.

   d. In the main display area, select Configure PIM-SM. PIM-SM configuration options now appear in the virtual router navigation tree under Dynamic Routing Protocol.


4. In the main display area, select the access list that identifies the permitted multicast group(s).

5. In the Group Specific Access Policies area, click the Add icon to map a multicast group to access lists. The Multicast Group IP dialog box appears.
a. Enter the IP address of the multicast group for which you created access lists for permitted RPs and permitted sources.

b. Select the ID of the access list that identifies the permitted RP(s). The device drops traffic for the multicast group if the traffic is from an RP that is not on the access list.

c. Select the ID of the access list that identifies the permitted source(s). This prevents unauthorized sources from sending data into your network. When you use this feature, the device drops multicast data from sources not in the list.

d. Click OK to save the new Multicast Group IP.

6. Click OK to save your changes to the virtual router, then click OK again to save your changes to the device configuration.

Configuring Proxy RP
You can configure a virtual router to function as a proxy RP. A proxy RP acts as the RP for groups learned from other zones. To configure a virtual router as a proxy RP, select Proxy when configuring the Rendezvous Point for PIM-SM.

EXAMPLE: CONFIGURING PIM
In this example, the hosts in the Trust zone are to receive the multicast stream for the multicast group 224.4.4.1/32. You configure RIP as the unicast routing protocol and create a firewall rule to pass data traffic between the Trust and Untrust zones. You create a PIM instance on the trust-vr and enable PIM on ethernet1 in the Trust zone, and on ethernet2 in the Untrust zone. ethernet1 is connected to the potential receivers; therefore, you also configure IGMP in router mode on this interface. You then create a multicast rule that permits PIM-SM BSR and join-prune messages between the zones.

1. Configure zones and interfaces.
   a. Configure ethernet1 and bind it to the Trust zone.
   b. Select IGMP in router mode on ethernet1, as shown below.

   Figure 42: Configure IGMP on an Interface

   c. Configure ethernet2 and bind it to the Untrust zone.

2. Configure the following address objects:
   - Multicast group IP address, as shown below:
3. Configure the access list that permits traffic from multicast group 224.4.4.1 (shown below).

4. Configure RIP.
   a. Create a RIP instance on the trust-vr, as shown below.

5. Configure PIM-SM.
   a. Create a PIM-SM instance on the trust-vr.
   b. Select Enable in the Parameters screen.
   c. Select PIM-SM on ethernet1 and on ethernet3, as shown below.
6. Configure a firewall rule that permits unicast and multicast data traffic to pass between zones, as shown below.

7. Configure a multicast rule permitting PIM-SM messages to pass between zones, as shown below.

---

**Configuring Multicast Route Table Entries**

Use static multicast routes to forward multicast data from the hosts on interfaces in IGMP router proxy mode to the routers upstream on the interfaces in IGMP host mode. (For information on IGMP proxy, see “Configuring IGMP Proxy” on page 204.)

**Configuring Multicast Routing Table Preferences**

You can configure the following settings for the multicast routing table:

- Enable Multiple Incoming Interfaces—Select this option to permit multiple routes with different incoming interfaces for the same source and multicast group.
Maximum Entries—Enter the maximum number of route entries you want the multicast routing table to hold. By default, this option is set to 4096.

Negative Mroute Cache—Select this option to store unroutable multicast packets in a cache until a multicast route can be established for the packet. For example, the security device might be unable to immediately route a multicast packet when:

- The IGMP proxy receives a data packet for which it has no interested member. The device creates a negative mroute entry for the packet and stores the packet in the negative mroute cache. When the IGMP proxy receives a group join for the source (or source and group), the device automatically forwards the cached packet.

- The device receives a data packet from a locally connected PIM-SM, but does not have a group RP mapping for that group. The device creates a negative mroute entry for the packet and stores the packet in the negative mroute cache. When the device learns the RP mapping, it automatically registers and forwards the packet.

- In an Active-Active NSRP configuration, the device that is not responsible for forwarding packets receives a multicast data packet. The device creates a negative mroute entry for the packet and stores the packet in the negative mroute cache. When the device that is responsible for forwarding packets learns of the group interest for the data packet, it forwards the packet.

When you enable Negative Mroute Cache, you can also configure a Timer that controls how the device ages unroutable packets in the cache. By default, the Timer is set to 90 seconds, meaning that the device deletes a route entry in the cache after 90 seconds. The acceptable range is 10 to 180 seconds.

Configuring a Multicast Static Route

For each static entry in the multicast routing table, you must configure the following information:

- Multicast Group IP—Enter the IP address of the group that receives multicast traffic.

- Source IP—Enter the IP address of the source of the multicast traffic.

- Incoming Interface—Select the interface on the device that receives multicast traffic.

- Outgoing Information—Enter the information that defines the interface and IP address the device uses to forward multicast traffic.

  - Outgoing Interface. Select the interface on the device that forwards multicast traffic.
Outgoing Group. Security devices can translate the original multicast group address to a different multicast group address on the outgoing interface. Use this option to specify the translated multicast group address for the outgoing interface (you configure the original group address in the Multicast Group IP setting).

You can configure multiple Outgoing Information settings for a single static multicast route.

EXAMPLE: CONFIGURING A STATIC MULTICAST ROUTE ENTRY
In this example, you configure a static multicast route from a source with IP address 20.20.20.200 to the multicast group 238.1.1.1. Configure the security device to translate the multicast group from 238.1.1.1 to 238.2.2.1 on the outgoing interface.

1. In the navigation tree, select Device Manager > Security Devices. Double-click the device object to open the device configuration.

2. In the device navigation tree, select Network > Virtual Router to display the list of configured virtual routers. Double-click the virtual router in which you are configuring a static multicast routing entry. The Virtual Router configuration screen appears.

3. In the virtual router navigation tree, select Multicast Routing Table. Configure the multicast routing preferences:
   a. Select Enable Multiple Incoming Interfaces.
   b. Select the Negative Mroute Cache. Leave the default Timer setting of 4096.

4. In the Multicast Static Routes area, click the Add icon. The New Mgroup dialog box appears. Configure the new routing entry:
   a. For Multicast Group IP, enter 238.1.1.1.
   b. For Source IP, enter 20.20.20.200.
   c. For Incoming Interface, select ethernet1.

5. Configure an Outgoing Information setting:
   a. Click the Add icon. The New Outgoing Information dialog box appears.
   b. For outgoing interface, select ethernet3.
   c. For Outgoing Group, enter the IP address 238.2.2.1.
   d. Click OK to add the Outgoing Information setting to the static route settings. Repeat step 5 to add more Outgoing Information settings.

6. Click OK to save your changes to the virtual router, then click OK again to save your changes to the device.
Configuring Zones

Use the Zone screen to configure predefined zones or create user-defined security zones. You can also create a tunnel zone, a logical segment to which a VPN tunnel interface is bound.

You can configure two types of zones on a security device:

- **A Security Zone**—A layer 3 security zone is a zone that binds to NAT or Route mode interfaces; a layer 2 security zone is a zone that binds to Transparent mode interfaces.

- **A tunnel zone** is a zone that binds to carrier zone.

To add a zone to a security device, in the device navigation tree, select Network > Zones and add the desired zone. For Security Zones, you might define the name of the zone and the virtual router in which you want to place the zone; for tunnel zones, you must also specify the carrier zone, which is the security zone with which the tunnel zone is logically associated. A carrier zone provides firewall protection to the encapsulated traffic.

For more detailed information about zones on security devices, see the “Fundamentals” volume in the NetScreen Concepts & Examples ScreenOS Reference Guide.

You can configure the following zone parameters for predefined or custom Security Zones:

- **Configuring Zone General Properties**
- **Configuring SCREEN Attack Protection**

**Configuring Zone General Properties**

For predefined zones, some general properties are already configured for you, such as the Name and Virtual Router settings. For custom security zones, you can enter a name and select the virtual router that handles traffic to and from the new zone.

For both predefined and custom zone, you can also configure the following settings:

- **TCP/IP Reassembly for ALG**—Select this option when using application layer gateway (ALG) filtering on the security device. By reassembling fragmented IP packets and TCP segments, the security device can accurately filter traffic.

- **Block Intrazone Traffic**—Select this option to block traffic between hosts within the security zone.

- **TCP-RST**—Select this option to return a TCP segment with the RESET flag set to 1 when a TCP segment with a flag other than SYN is received.
Asymmetric VPN—In asymmetrical encryption, one key in a pair is used to encrypt and the other to decrypt VPN traffic. When configuring multiple VPN tunnels to enable tunnel failover, enable this option for the Trust zones on each security device in the VPN so that if an existing session established on one VPN tunnel transfers to another, the security device at the other end of the tunnel does not reject it.

Configuring SCREEN Attack Protection

Typically, a network forwarding device such as a router or switch does not reassemble fragmented packets that it receives. It is the responsibility of the destination host to reconstruct the fragmented packets when they all arrive. Because the purpose of forwarding devices is the efficient delivery of traffic, queuing fragmented packets, reassembling them, then refragmenting them, and forwarding them is unnecessary and inefficient. However, passing fragmented packets through a firewall is insecure. An attacker can intentionally break up packets to conceal traffic strings that the firewall otherwise would detect and block.

You can enable predefined screen options that detect and block various kinds of traffic that the security device determines to be potentially harmful. To secure all connection attempts, security devices use a dynamic packet filtering method known as stateful inspection. Using this method, the device notes various components in a packet header, such as source and destination IP addresses, source and destination port numbers, and packet sequence numbers. The device uses this information to maintain the state of each session traversing the firewall.

A security device uses stateful inspection to secure a zone by inspecting, and then permitting or denying, all connection attempts that require crossing an interface from and to that zone. To protect against attacks from other zones, you can enable defense mechanisms known as screen attack protections, which detect and deflect TCP, UDP, IP, and ICMP packet attacks. Common Screen attacks are SYN floods, packet fragments, and SYN and FIN bits set. When Screen attack protections are enabled, the device generates a screen alarm log entry for each violation.

To configure Screen attack protections, open a device configuration and select Network > Zones to display the Zone configuration. Double-click a zone to display the Predefined Zone dialog box and select SCREEN.

NOTE: For step-by-step instructions on configuring the SCREEN options, see the NetScreen-Security Manager Online Help topic “Configuring SCREEN Options”. For details on the SCREEN alarm log entries that enabling these options can generate, see “Screen Alarm Log Entries” on page 836.

Defending Against Floods

Configure flood defense settings to prevent denial-of-service (DoS) attacks from overwhelming the security device with large numbers or floods of certain packet types. You can protect targets in the security zone from ICMP, SYN, and UDP floods.
Configuring ICMP Flooding Protection
An ICMP flood occurs when incoming ICMP echo requests overload a target system with so many requests that the system expends all its resources responding until it can no longer process valid network traffic. You can protect targets in the security zone from ICMP floods by setting a packet-per-second threshold for ICMP requests (default setting: 1000 packets/sec). When the ICMP packet flow exceeds the defined threshold, the security device ignores further ICMP echo requests for the remainder of that second plus the next second as well.

Configuring SYN Flooding Protection
A SYN flood occurs when a target becomes so overwhelmed by SYN segments initiating uncompletable connection requests that it can no longer process legitimate connection requests. You can configure thresholds for the zone that, when exceeded, prompt the security device to begin proxying incoming SYN segments, replying with SYN/ACK segments, and storing the incomplete connection requests in a connection queue. The incomplete connection requests remain in the queue until the connection is completed or the request times out.

To protect targets in the security zone from SYN floods, enable SYN Flood Protection and configure the following thresholds for SYN segments passing through the zone:

- **Threshold**—Configure the number of SYN packets (TCP segments with the SYN flag set) per second required for the security device to begin SYN proxy. This threshold is the total number of packets passing through the zone, from all sources to all destinations.

- **Alarm Threshold**—Configure the number of proxied TCP connection requests required to generate an alarm in an alarm log entry for the event.

- **Source Threshold**—Configure the number of SYN packets per second from a single IP address required for the security device to begin rejecting new connection requests from that source.

- **Destination Threshold**—Configure the number of SYN packets per second to a single IP address required for the security device to begin rejecting new connection requests to that destination.

- **Timeout Value**—Configure the number of seconds the security device holds an incomplete TCP connection attempt in the proxied connection queue.

- **Queue Size**—Configure the number of proxied TCP connection requests held in the proxied connection queue before the security device begins rejecting new connection requests.
Configuring UDP Flooding Protection

Security devices currently support UDP for incoming SIP calls. To protect targets in the security zone against UDP flooding by incoming SIP traffic, enable UDP Flooding Protection. The security device can limit the number of UDP packets that can be received by an IP address, preventing incoming SIP calls from overwhelming the target.

SIP signaling traffic consists of request and response messages between client and server and uses transport protocols such as UDP or TCP. The media stream carries the data (for example, audio data), and uses application layer protocols such as RTP (Real-time Transport Protocol) over UDP.

EXAMPLE: CONFIGURING UDP FLOOD PROTECTION BY LIMITING UDP PACKETS
In this example, enable UDP Flooding Protection and set a threshold of 80000 per second for the number of UDP packets that can be received on IP address 1.1.1.5, in the Untrust zone. When this limit is reached, the device generates an alarm and drops subsequent packets for the remainder of that second.

1. Add a NetScreen-208 security device. Choose Model when adding the device and configure the device as running ScreenOS 5.1 or higher.

2. In the device navigation tree, select Network > Zone. Double-click the Untrust zone. The General Properties screen appears.

3. In the zone navigation tree, select Screen > Flood Defense, then click the UDP Flood Defense tab.

4. Select UDP Flood Protection and ensure that the Threshold is set to 1000.

5. Click the Add icon to display the New Destination IP based UDP Flood Protection dialog box. Configure the following, then click OK:
   - For Destination IP, enter 1.1.1.5.
   - For Threshold, enter 80000.

6. Click OK to save your changes to the zone, then click OK again to save your changes to the device.

Blocking HTTP Components

Attackers may use HTTP to send ActiveX controls, Java applets, .zip files, or .exe files to a target system, enabling them to load and control applications on hosts in a protected network. You can configure the security device to block the following components (the device monitors incoming HTTP headers for blocked content types):
Java—Java applets enable Web pages to interact with other programs. The applet runs by downloading itself to the Java Virtual Machine (VM) on a target system. Because attackers can program Java applets to operate outside the VM, you might want to block them from passing through the security device.

ActiveX—Microsoft's ActiveX enables different programs to interact with each other, and might contain Java applets, .exe file, or .zip files. Web designers use ActiveX to create dynamic and interactive Web pages that function similarly across different OSes and platforms. However, attackers may also use ActiveX to gain control over a target computer system. When blocking ActiveX components, the security device also blocks Java applets, .exe files, and .zip files whether they are contained within an ActiveX control or not.

ZIP files—Files with .zip extensions contain one or more compressed files, some of which might be .exe files or other potentially malicious files. You can configure the security device to block all .zip files from passing through the zone.

EXE files—Files with .exe extensions might contain malicious code. You can configure the security device to block all .exe files from passing through the zone.

Configuring MS-Windows Defense
Microsoft Windows contains the WinNuke vulnerability, which can be exploited using a DoS attack targeting any computer on the Internet running Microsoft Windows. Attackers can send a TCP segment (usually to NetBIOS port 139 with the urgent (URG) flag set) to a host with an established connection; this packet causes a NetBIOS fragment overlap that can crash Windows systems.

To protect targets in the security zone from WinNuke attacks, configure the security device to scan incoming Microsoft NetBIOS session service (port 139) packets for set URG flags. If such a packet is detected, the security device unsets the URG flag, clears the URG pointer, forwards the modified packet, and generates a log entry for the event.

Defending Against Scans, Spoofs, and Sweeps
Attackers often perform address sweeps and/or port scans to gain targeted information about a network. After they have identified trusted addresses or ports, they might launch an attack against the network by spoofing a trusted IP address. To protect targets in the zone from sweeps, scans, and spoofing attempts, configure the following detection and blocking settings:

IP Address Spoof Protection—Attackers can insert a bogus source address in a packet header to make the packet appear to come from a trusted source. When the interfaces in the zone operate in Route or NAT mode, the security device relies on route table entries to identify IP spoofing attempts. When the interfaces in the zone operate in Transparent mode, the security device relies on address book entries to identify IP spoofing attempts.

To enable interface-based IP spoofing protection, configure the security device to drop packets whose source IP addresses do not appear in the route table.
To enable zone-based IP spoofing protection (supported on devices running ScreenOS 5.2), configure the security device to drop packets whose source IP addresses do not appear in the selected zone. If you are routing traffic between two interfaces in the same zone, you should leave this option disabled (unchecked).

IP Address Sweep Protection—An address sweep occurs when one source IP address sends 10 ICMP packets to different hosts within a defined interval. If a host responds with an echo request, attackers have successfully discovered a target IP address. You can configure the security device to monitor ICMP packets from one remote source to multiple addresses. For example, if a remote host sends ICMP traffic to 10 addresses in 0.005 seconds (5000 microseconds), the security device rejects the 11th and all further ICMP packets from that host for the remainder of that second.

Port Scan Protection—A port scan occurs when one source IP address sends IP packets containing TCP SYN segments to 10 different ports at the same destination IP address within a defined interval (5000 microseconds is the default). If a port responds with an available service, attackers have discovered a service to target. You can configure the security device to monitor TCP SYN segments from one remote source to multiple addresses. For example, if a remote host scans 10 ports in 0.005 seconds (5000 microseconds), the security device rejects all further packets from the remote source for the remainder of that second.

Configuring IP Option Anomaly Detection

The Internet Protocol standard “RFC 791, Internet Protocol” specifies a set of eight options that provide special routing controls, diagnostic tools, and security. Attackers can misconfigure these IP options to evade detection mechanisms and/or perform reconnaissance on a network.

To detect (and block) anomalous IP fragments as they pass through the zone, configure the following settings:

- Block Bad IP Options—Select this option to block packets with an IP datagram header that contains an incomplete or malformed list of IP options.

- Timestamp IP Option Detection—Select this option to block packets in which the IP option list includes option 4 (Internet Timestamp). The timestamp option records the time when each network device receives the packet during its trip from the point of origin to its destination, as well as the IP address of each network device and the transmission duration of each one. If the destination host has been compromised, attackers can discover the network topology and addressing scheme through which the packet passed.

- Security IP Option Detection—Select this option for hosts to send security, compartmentation, TCC (closed user group) parameters, and Handling Restriction Codes compatible with U.S. Department of Defense requirements.

- Stream IP Option Detection—Select this option to block packets in which the IP option is 8 (Stream ID). Packets must use the 16-bit SATNET stream identifier to be carried through networks that do not support the stream concept.
- Record Route IP Option Detection—Select this option to block packets in which the IP option is 7 (Record Route). Attackers may use this option to record the series of Internet addresses through which a packet passes, enabling them to discover network addressing schemes and topologies.

- Loose Source IP Option Detection—Select this option to block packets in which the IP option is 3 (Loose Source Routing). The Loose Source Routing option enables the packet to supply routing information used by the gateways when forwarding the packet to the destination; the gateway or host IP can use any number of routes from other intermediate gateways to reach the next address in the route.

- Strict Source IP Option Detection—Select this option to block packets in which the IP option is 9 (Strict Source Routing). The Strict Source Routing enables the packet to supply routing information used by the gateways when forwarding the packet to the destination; the gateway or host IP must send the datagram directly to the next address in the source route, and only through the directly connected network indicated in the next address to reach the next gateway or host specified in the route.

- Source Route IP Option Filter—Select this option to block all IP traffic that contains the Source Route option. The Source Route option enables the IP header to contain routing information that specifies a different source than the header source. Attackers can use the Source Route option to send a packet with a phony source IP address; all responses to the packet are sent to the attacker’s real IP address.

Configuring TCP/IP Anomaly Protection

Attackers can craft malicious packets (and packet fragments) that contain anomalies designed to bypass detection mechanisms and gain targeted information about a network. Because different OSes respond differently to anomalous packets, attackers can determine the OS running on a target by examining the target’s response to the packet. To protect targets in the security zone from these reconnaissance attempts, you can configure the following settings:

- SYN Fragment Detection—Select this option to detect TCP fragments that contain a SYN flag. A SYN flag in TCP segment initiates a connection, but does not usually contain a payload. Because the packet is small, it should not be fragmented.

- Drop Packet without TCP Flags Set—Select this option to detect TCP segment headers that do not have at least one flag control set.

- Block SYN with FIN TCP Segments—Select this option to detect packets in which both the SYN and FIN flags are set. The SYN flag synchronizes sequence numbers to initiate a TCP connection and the FIN flag indicates the end of data transmission to finish a TCP connection, so both flags should never be set in the same packet.

- Block FIN without ACK TCP Segments—Select this option to detect packets in which the FIN flag is set but the ACK flag is not. The FIN flag signals the conclusion of a session and terminates the connection; normally the ACK flag is also set to acknowledge the previous packet received.
Drop Packets with an Unknown Protocol—Select this option to drop packets in which the protocol field is set to 101 or greater. Protocol types 101 and higher are currently reserved and undefined.

Denial of Service Defense

Attackers use denial-of-service (DoS) attacks to overwhelm a target with traffic from a single source IP, preventing the target from processing legitimate traffic. A more advance version of DoS is the distributed denial-of-service (DDoS), in which attackers use multiple source addresses. Typically, attackers use a spoofed IP address or a previously compromised IP address as the source address to avoid detection.

To protect targets in the security zone from DoS and DDoS attacks, configure the following settings:

- Ping of Death Attack Protection—Select this option to reject oversized and irregular ICMP packets. Attackers may send a maliciously crafted ping (ICMP packet) that is larger than the allowed size of 65,507 bytes to cause a DoS.

- Teardrop Attack Protection—Select this option to drop teardrop attack packets, designed to exploit vulnerabilities in the reassembly of fragmented IP packets. In the IP header, the fragment offset field indicates the starting position, or “offset”, of the data contained in a fragmented packet relative to the data of the original unfragmented packet. When the sum of the offset and size of one fragmented packet differ from that of the next fragmented packet, the packets overlap, and the server attempting to reassemble the packet can crash.

- Block ICMP Fragments—Select this option to block ICMP packets with the More Fragments flag set, or with an offset value in the offset field. ICMP packets are typically very short messages containing error reports or network probe information. Because ICMP packets do not carry large payloads, they should not be fragmented.

- Block Large ICMP Packets—Select this option to block ICMP packets larger than 1024 bytes. ICMP packets are typically very short messages containing error reports or network probe information; a large ICMP packet is suspicious.

- Block IP Packet Fragments—Select this option to block IP fragments destined for interfaces in the security zone. As packets traverse different networks, it is sometimes necessary to break a packet into smaller pieces (fragments) based upon the maximum transmission unit (MTU) of each network. Attackers can use IP fragments to exploit vulnerabilities in the packet reassembly code of specific IP stack implementations.

- Land Attack Protection—Select this option to block SYN floods and IP spoofing combinations. Attackers can initiate a Land attack by sending spoofed SYN packets that contain the IP address of the target as both the destination and source IP address. The target responds by sending the SYN-ACK packet to itself, creating an empty connection that lasts until the idle timeout value is reached; in time, these empty connections overwhelm the system.
SYN-ACK-ACK Proxy Protection—Select this option and configure a threshold to prevent SYN-ACK-ACK sessions from flooding the security device session table. After successfully receiving a login prompt from the security device, attackers can continue initiating SYN-ACK-ACK sessions, flooding the security device session table and causing the device to reject legitimate connection requests. When proxy protection is enabled and the number of connections from the same IP address reaches the SYN-ACK-ACK proxy threshold, the security device rejects further connection requests from that IP address. By default, the threshold is 512 connections from any single IP address; you can customize this threshold (1 to 250,000) to meet your networking requirements.

Source IP-Based Session Limit—Select this option and configure a threshold to limit the number of concurrent sessions from the same source IP address. The default threshold is 128 sessions; you can customize this threshold to meet your networking requirements.

Destination IP-Based Session Limit—Select this option and configure a threshold to limit the number of concurrent sessions to the same destination IP address. The default threshold is 128 sessions; you can customize this threshold to meet your networking requirements.

Configuring Mal URL Protection
Enable malicious URL protection on a security device to drop incoming HTTP packets that reference URLs with specific user-defined patterns. You can define up to 48 malicious URL string patterns per zone, each of which can be up to 64 characters long, for malicious URL protection at the zone level. When the Malicious URL blocking feature is selected, the security device examines the data payload of all HTTP packets. If it locates a URL and detects that the beginning of its string—up to a specified number of characters—matches the pattern you defined, the device blocks that packet from passing the firewall.

A resourceful attacker, realizing that the string is known and might be guarded against, can deliberately fragment the IP packets or TCP segments to make the pattern unrecognizable during a packet-by-packet inspection. However, security devices use Fragment Reassembly to buffer fragments in a queue, reassemble them into a complete packet, and then inspect that packet for a malicious URL. Depending on the results of this reassembly process and subsequent inspection, the device performs one of the following steps:

- If the device discovers a malicious URL, it drops the packet and enters the event in the log.
- If the device cannot complete the reassembly process, a time limit is imposed to age out and discard fragments.
- If the device determines that the URL is not malicious but the reassembled packet is too big to forward, the device fragments that packet into multiple packets and forwards them.
- If the device determines that the URL is not malicious and does not need to fragment it, it then forwards the packet.

To configure a malicious URL string, you must specify the following properties:
Malicious URL ID—Enter the ID that you want use to identify the URL string.

HTTP Header Pattern—Enter the malicious URL string (also called a pattern) that you want the security device to match.

Minimum Length Before CRLF—Enter the number of characters in the URL string (pattern) that must be present in a URL—starting from the first character—for a positive match (not every character is required for a match). CRLF represents “carriage return/line feed”; HTTP uses a CR or LF character to mark the end of a code segment.

For more detailed information about Mal-URL on security devices, see the “Attack Detections and Defense Mechanisms”, volume 4 in the NetScreen Concepts & Examples ScreenOS Reference Guide.

EXAMPLE: BLOCKING MALICIOUS URLS IN PACKET FRAGMENTS

In this example, you define three malicious URL strings and enable the malicious URL blocking option. Then, enable fragment reassembly for the detection of the URLs in fragmented HTTP traffic arriving at an Untrust zone interface.

1. Add a NetScreen-5GT security device. Choose Model when adding the device and configure the device as running ScreenOS 5.x.

2. In the device navigation tree, select Network > Zone. Double-click the Untrust zone. The General Properties screen appears.

3. Select TCP/IP Reassembly for ALG.

4. In the Zone navigation tree, select Mal-URL. Configure the three malicious URL strings:
   a. Click the Add icon to display the new Malicious URL ID dialog box. Configure the following and click OK:
      - For Malicious URL ID, enter Perl.
      - For HTTP Header Pattern, enter scripts/perl.exe.
      - For Minimum Length Before CRLF, enter 14.
   b. Click the Add icon to display the new Malicious URL ID dialog box. Configure the following and click OK:
      - For Malicious URL ID, enter CMF.
      - For HTTP Header Pattern, enter cgi-bin/phf.
      - For Minimum Length Before CRLF, enter 11.
   c. Click the Add icon to display the new Malicious URL ID dialog box. Configure the following and click OK:
      - For Malicious URL ID, enter DLL.
      - For HTTP Header Pattern, enter 210.1.1.5/msadcs.dll.
For Minimum Length Before CRLF, enter 18.

5. Click OK to save your changes to the zone, then click OK again to save the device configuration.

Configuring UDP Flooding Protection

Security devices currently support UDP for incoming SIP calls. To protect the managed device against UDP flooding by incoming SIP traffic, enable UDP Flooding Protection. The device can limit the number of UDP packets that can be received by an IP address, preventing incoming SIP calls from overwhelming the device.

SIP signaling traffic consists of request and response messages between client and server and uses transport protocols such as UDP or TCP. The media stream carries the data (for example, audio data), and uses application layer protocols such as RTP (Real-time Transport Protocol) over UDP.

EXAMPLE: CONFIGURING UDP FLOOD PROTECTION BY LIMITING UDP PACKETS
In this example, enable UDP Flooding Protection and set a threshold of 80000 per second for the number of UDP packets that can be received on IP address 1.1.1.5, in the Untrust zone. When this limit is reached, the device generates an alarm and drops subsequent packets for the remainder of that second.

1. Add a NetScreen-208 security device. Choose Model when adding the device and configure the device as running ScreenOS 5.1.

2. In the device navigation tree, select Network > Zone. Double-click the Untrust zone. The General Properties screen appears.

3. In the zone navigation tree, select Screen > Flood Defense, then click the UDP Flood Defense tab.

4. Select UDP Flood Protection and ensure that the Threshold is set to 1000.

5. Click the Add icon to display the New Destination IP based UDP Flood Protection dialog box. Configure the following, then click OK:
   - For Destination IP, enter 1.1.1.5.
   - For Threshold, enter 80000.

6. Click OK to save your changes to the zone, then click OK again to save your changes to the device.

Configuring Interfaces

The Interface screen displays the physical interfaces available on the security device. Some security devices support function zone interfaces, which are either a separate physical MGT interface for management traffic or a high availability (HA) interface used to link two devices together to form a redundant group or cluster.

NOTE: UDP Flood Protection appears only for devices running ScreenOS 5.1 and higher.
Interfaces and subinterfaces enable traffic to enter and exit a security zone. To enable network traffic to flow in and out of a security zone, you must bind an interface to that zone and, if it is a Layer 3 zone, assign it an IP address. You can assign multiple interfaces to a zone, but you cannot assign a single interface to multiple zones.

**Interface Types**

You can add the following interfaces on a security device:

- **Aggregate interface**—A logical interface that combines two or more physical interfaces on the device, for the purpose of share the traffic load to a single IP address. This type of interface is only supported on certain security device systems.

- **Multilink interface**—On an SSG 520/550 security device, you configure and access multiple serial links called a bundle, through a virtual interface called a multilink interface. The multilink interface emulates a physical interface for the transport of frames.

- **Loopback interface**—A logical interface that emulates a physical interface and is always in the up state.

- **Virtual security interfaces (VSIs)**—The virtual interfaces that two security devices share when forming a virtual security device (VSD) in a high availability cluster.

- **Redundant interface**—Consists of two physical interfaces bound to the same security zone. One of the two physical interfaces acts as the primary interface and handles all the traffic directed to the redundant interface; the other physical interface acts as a backup.

- **Subinterface**—A logical division of a physical interface. A subinterface borrows the bandwidth it needs from the physical interface.

- **Tunnel interface**—Acts as a doorway to a VPN tunnel. Traffic enters and exits a VPN tunnel via a tunnel interface. When you configure a tunnel interface, you can also encapsulate IP multicast packets in GREv1 unicast packets.

- **ADSL interface**—A NetScreen-5GT ADSL security device uses ATM as its transport layer. The interface can support multiple permanent virtual circuits (PVCs) on a single physical line. Before you can configure the adsl1 interface, however, you must obtain the DSLAM configuration details for the ADSL connection from the service provider.

- **WAN Subinterface**—A logical division of a physical WAN interface. This type of interface is only supported on SSG 520 and 550 security devices.

- **Wireless interface**—A NetScreen-5GT Wireless security device interface handles wireless traffic to and from that wireless access point (WAP).

For details and examples on configuring specific interface types, see “Interface Configuration Examples” on page 252.
Configuring Physical and Function Zone Interfaces

In the Interface screens, you can configure the physical interfaces and, if available, the function zone interfaces. Double-click the interface in the Interface screen (or, either select the interface and then click the Edit icon, or right-click the interface and select Edit). For physical and function zone interfaces, you can configure the following:

- Configuring Interface General Properties
- Configuring WAN Properties
- Configuring Port Properties
- Configuring MLFR and MLPPP Options
- Configuring Interface Advanced Properties
- Configuring Interface Service Options
- Configuring DHCP
- Configuring Interface Protocol
  - For details on configuring dynamic routing protocols (BGP, RIP, OSPF) in the virtual router and on the interfaces, see “Configuring Dynamic Routing” on page 186.
  - For details on configuring multicast routing protocols (PIM-SIM, IGMP, IGMP-Proxy) and multicast route entries, see “Configuring Multicast Routing” on page 202
- Configuring Interface Secondary IP
- Configuring Interface Monitoring
- Configuring GRE
- Configuring Interface NAT

For more detailed explanations about interfaces on security devices, see the “Fundamentals” volume in the NetScreen Concepts & Examples ScreenOS Reference Guide.

Configuring Interface General Properties
Use the General Properties screen to set the following properties on an Interface:

- Name of the interface
- Sub Interface Type
- Zone to which the interface is bound
- VLAN tag
- Bundle into—used to configure virtual interfaces on a Multilink Frame Relay (MLFR) for User-to-Network Interface (UNI) (only available on SSG 520 and 550 security devices).

- Encapsulation Type—used to configure the following encapsulation protocols on WAN interfaces: Frame Relay, Multilink Frame Relay (MLFR), Point-to-Point Protocol (PPP), Multilink PPP (MLPPP), and Cisco High-Level Data Link Control (HDLC) (only available on SSG 520 and 550 security devices).

- Loopback interface group to which the interface belongs

- Redundant interface group to which the interface belongs

- IP address, netmask, and gateway of the interface

**NOTE:** NetScreen-Security Manager does not permit you to unset the management IP Address. You can however, still do this on each separate device out of band, using CLI, WebUI or the Supplemental CLI. Refer to “Configuring Supplemental Command Line Interface (CLI)” on page 348 for more information.

- Mode of the interface (NAT or route)

- Select DNS Proxy (for details, see “Configuring DNS Proxy” on page 292.)

- PPP Settings

On security device ADSL interfaces, you can also configure ADSL options (VPI, VCI, Multiplexing mode) as part of the General Properties for the ADSL interface. For details on configuring ADSL, see “Configuring an ADSL Interface” on page 264.

On wireless interfaces, you can also shutdown the interface by enabling the option “Shutdown Interface.”

On some security device interfaces, such as the VLAN1 or Serial interface, you also configure the service options as part of the General Properties for the interface. For details on service options, see “Configuring Interface Service Options” on page 228.

**Configuring WAN Properties**

Use the WAN Properties screen to configure the following WAN properties for port cards on the SSG 520 and 550 only:

- Clocking

- Hold Time (Up)

- Hold Time (Down)

For more information on configuring WAN properties for port cards on the SSG 520 and 550 security device, refer to the ScreenOS Wide Area Network Interfaces and Protocols Reference.
Configuring Port Properties

Use the Port Properties screen to configure the following properties for port cards on the SSG 520 and 550 only:

- Port Configuration (Serial, E1, T1, or DS3)
- DCE Options
- DTE Options
- Line encoding
- Loopback mode
- Encapsulation support

For more information on configuring properties for port cards on the SSG 520 and 550 security device, refer to the ScreenOS Wide Area Network Interfaces and Protocols Reference.

Configuring MLFR and MLPPP Options

Use the MLFR and MLPPP screens to change the default frame relay and PPP properties on a multilink interface. For more information on configuring frame relay properties on the SSG 520 and 550 security device, refer to the ScreenOS Wide Area Network Interfaces and Protocols Reference.

Configuring Interface Advanced Properties

Set attributes of the physical link for the interface:

- Physical Settings
  - Extended Bandwidth Settings. Use the Egress Bandwidth options to set the minimum (or guaranteed) and maximum bandwidth allowed to pass through the security device. Be careful not to allocate more bandwidth than the interface can support, as you may lose data if the guaranteed bandwidth on contending policies surpasses the traffic bandwidth set on the interface.

  For security devices running ScreenOS 5.3, you can also manage the flow of traffic through the security device by limiting bandwidth at the point of ingress. To configure the maximum amount of traffic allowed at the point of the ingress interface, set the number of kilobits per second (kbps) using the Ingress Minimum Bandwidth field.

  Refer to “Configuring Traffic Shaping” on page 337 for more information on configuring traffic shaping parameters on the device.

  Holddown Time. Use this option to configure the amount of time (in milliseconds) that the security device uses to bring the interface up or down after detecting a change in the link status.
- Bring Down Link. Select this option to bring down the physical link to the interface.

- Link and MTU Size.

- WebAuth.
  - Enable Webauth. Select this option to enable device administrators to authenticate management connections to the device using WebAuth.
  - WebAuth IP. Enter the IP address of the WebAuth service on the interface.
  - Allow Webauth via SSL only (ScreenOS 5.1 and higher Only). Select this option to require WebAuth users to use SSL when connecting to the WebAuth IP address on a device running ScreenOS 5.1 and higher. When this option is disabled, device administrators can access the WebAuth IP address of the interface using clear text.

**NOTE:** When you enable WebAuth, you must also enable SSL as a service option for the interface. For details, see "Configuring Interface Service Options" on page 228.

- Deny Routing

- Port Settings

### Configuring Interface Service Options
Enable management service options for the interface:

- Web—Selecting this option enables the interface to receive HTTP traffic for management from the Web user interface (WebUI).

- Telnet—A terminal emulation program for TCP/IP networks such as the Internet, Telnet is a common way to remotely control network devices. Selecting this option enables Telnet manageability.

- SSH—You can administer the security device from an Ethernet connection or a dial-in modem using Secure Command Shell (SSH). You must have an SSH client that is compatible with Version 1.5 of the SSH protocol. These clients are available for Windows 95 and later, Windows NT, Linux, and UNIX. The security device communicates with the SSH client through its built-in SSH server, which provides device configuration and management services. Selecting this option enables SSH manageability.

- SNMP—The security device supports both SNMPv1 and SNMPv2c, and all relevant Management Information Base II (MIB II) groups, as defined in RFC-1213. Selecting this option enables SNMP manageability.

- SSL—Select this option to enable the interface to receive HTTPS traffic for secure management of the security device using the WebUI. Additionally, when this option is enabled, you can also require WebAuth users to use SSL when connecting to the WebAuth IP address on a device running ScreenOS 5.1 and higher.
Global Pro (Security Manager)—Selecting this option enables the interface to receive NetScreen-Security Manager traffic.

Ping—Selecting this option enables the interface to respond to an ICMP echo request, or ping, which determines whether a specific IP address is accessible over the network.

Ident-Reset—Services like Mail and FTP send identification requests. If they receive no acknowledgement, they send the request again. While the request is processing, there is no user access. By enabling the Ident-reset option, the interface sends a TCP reset announcement in response to an IDENT request to port 113 and restores access that has been blocked by an unacknowledged identification request.

NSGP—Select this option to enable the interface to handle NSGP traffic. When enabled, you can also select to enforce IPSec authentication for NSGP traffic.

Configuring DHCP
The Dynamic Host Configuration Protocol (DHCP) automatically assigns TCP/IP settings for the hosts on the network. Different security devices support different DHCP roles:

- DHCP clients receive a dynamically assigned IP address.
- DHCP servers allocate dynamic IP addresses to clients.
- DHCP relay agents receive information from a DHCP server and relay that information to clients.

Some devices can simultaneously act as a DHCP client, server, and relay agent.

Configuring Custom DHCP Options
When configuring a DHCP server, you can also configure custom DHCP options to handle address assignment for Voice-over-IP (VOIP) phones.

A custom DHCP option contains:

- Option Name—The option name is a user-defined, unique name that identifies the custom option.

- Code—The option code is an arbitrary integer that represents the option type. Use the option code to represent the custom option you want to configure. For each DHCP server, you can configure an unlimited number of custom DHCP options; however, the option code for each custom option must be unique, and cannot match the option code for a predefined option (DHCP contains several predefined option codes). The following table details all predefined option codes as well as the RFC2132 term for that option code:

---

NOTE: Custom DHCP options are not supported on the NetScreen-500, the NetScreen-5200, the NetScreen-5400, the ISG 1000 and the ISG 2000.
Table 12: Predefined DHCP Option Codes for DHCP Servers

<table>
<thead>
<tr>
<th>Options</th>
<th>Option Code (cannot be used for custom option code)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Netmask</td>
<td>1</td>
</tr>
<tr>
<td>Gateway</td>
<td>3</td>
</tr>
<tr>
<td>DNS1, DNS2, DNS3</td>
<td>6</td>
</tr>
<tr>
<td>Domain Name</td>
<td>15</td>
</tr>
<tr>
<td>WINS1, WINS2</td>
<td>44</td>
</tr>
<tr>
<td>Lease</td>
<td>51</td>
</tr>
<tr>
<td>SMTP</td>
<td>69</td>
</tr>
<tr>
<td>POP3</td>
<td>70</td>
</tr>
<tr>
<td>News</td>
<td>71</td>
</tr>
<tr>
<td>NIS1, NIS2</td>
<td>112</td>
</tr>
<tr>
<td>NIS TAG</td>
<td>113</td>
</tr>
</tbody>
</table>

In addition to predefined option codes, the codes 0, 255, and 53 cannot be used to create a custom DHCP option. All other integers between 2 and 254 are valid.

- **Data Type**—The data type controls the type of data required for the option code. Available data types are String, IP Address, and Integer.
- **Value**—The value of the option code. When the data type is string, the acceptable length is 1-128 characters.

**EXAMPLE: CONFIGURING CUSTOM OPTIONS FOR A DHCP SERVER**

Your network recently added support for VoIP, and you now need to support DHCP for Voice-over-IP (VoIP) phones. You edit the existing DHCP server configuration to send the following custom options to IP phones acting as DHCP clients:

- Option code 444, containing string “Server 4”
- Option code 66, containing IP address 1.1.1.1
- Option code 160, containing integer 2004

The example assumes that you have already configured a security device to act as a DHCP server.

1. In the main navigation tree, select Device Manager > Security Devices. Double-click the device currently handling your DHCP assignments.
3. In the interface navigation tree, select DHCP, set the DHCP mode to Server, then select the Custom Options tab.
4. Click the Add icon to add the first custom option. Configure the following, then click OK:
Chapter 5: Configuring Devices

- For Option Name, enter IP Address.
- For Code, enter 66.
- For Data Type, select IP ADDR.
- For Value, enter 1.1.1.1.

5. Click the Add icon to add the second custom option. Configure the following, then click OK:

- For Option Name, enter Server 4.
- For Code, enter 444.
- For Data Type, select STRING.
- For Value, enter Server 4.

6. Click the Add icon to add the third custom option. Configure the following, then click OK:

- For Option Name, enter Year 2004.
- For Code, enter 160.
- For Data Type, select INTEGER.
- For Value, enter 2004.

Your custom options should now appear as shown below:

Figure 49: View Custom Options for DHCP Server

<table>
<thead>
<tr>
<th>Server Settings</th>
<th>Custom Options</th>
<th>IP Pools</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Add icon]</td>
<td>![Modify icon]</td>
<td>![Delete icon]</td>
</tr>
<tr>
<td>Option Name</td>
<td>Code</td>
<td>Data Type</td>
</tr>
<tr>
<td>IP Address</td>
<td>66</td>
<td>IP ADDR</td>
</tr>
<tr>
<td>Server 4</td>
<td>444</td>
<td>STRING</td>
</tr>
<tr>
<td>Year 2004</td>
<td>160</td>
<td>INTEGER</td>
</tr>
</tbody>
</table>

7. Click OK to save your changes to the interface, then click OK again to save your changes to the device.

Configuring Interface Protocol

You can enable and configure dynamic routing protocol and multicast protocol operations on the interface:

- For details on configuring dynamic routing protocols (BGP, RIP, OSPF) in the virtual router and on the interfaces, see “Configuring Dynamic Routing” on page 186.
For details on configuring multicast routing protocols (PIM-SIM, IGMP, IGMP-Proxy) and multicast route entries, see “Configuring Multicast Routing” on page 202

Configuring Interface Secondary IP
This option is not available for interfaces in the Untrust zone. Each interface has a single, unique primary IP address. You can also set one or more secondary IP addresses for the interface.

Configuring Interface Monitoring
You can enable the security device to monitor the reachability of certain IP addresses through the interface to determine interface failure. For each IP address to be tracked, specify the following:

- Interval at which pings are sent to the tracked address
- Number of consecutive unsuccessful ping attempts before the connection to the address is considered failed
- Weight of the failed IP connection

The Failover Threshold is compared to the sum of the weights of failed IP connections. Instead of tracking specific IP addresses, you can alternatively set the device to track the interface’s default gateway.

Configuring GRE
You can configure a tunnel interface to support GREv1 encapsulation. When enabled, the interface encapsulates IP packets in the tunnel in IPv4 packets using the Generic Routing Encapsulation version 1 (GREv1) protocol. You must specify the key parameter to append the value to outgoing packets (incoming packets must have this value too).

You can use GRE to forward multicast packets through non-multicast aware routers and devices.

Configuring Interface NAT
You can configure the following address translation methods on the security device:

- Mapped IP (MIP) settings—For details on configuring a MIP, see “Configuring MIPs” on page 233.
- Dynamic IP (DIP) settings—For details on configuring a DIP, see “Configuring DIPs” on page 239. For details on DIP groups for security devices in an active/active NSRP configuration, see “Configuring DIP Groups” on page 276.
- Virtual IP (VIP) settings—For details on configuring a VIP, see “Configuring VIPs” on page 236.
Configuring MIPs

A mapped IP (MIP) is a direct one-to-one mapping of one IP address to another. The security device forwards incoming traffic destined for a MIP to the host with the address to which the MIP points. A MIP is static destination address translation that maps the destination IP address in an IP packet header to another static IP address, enabling inbound traffic to reach private addresses in a zone whose interface is in NAT mode. When a MIP host initiates outbound traffic, the security device translates the source IP address of the host to that of the MIP address. You can map an address-to-address or subnet-to-subnet relationship (the netmask applies to both the mapped IP subnet and the original IP subnet).

You can also use a MIP to handle overlapping address spaces at two sites connected by a VPN tunnel (an overlapping address space is when the IP address range in two networks are partially or completely the same).

The zone you configure the MIP in determines the subnet of IP address that you can assign the MIP:

- When defining a MIP in a tunnel zone or security zone other than untrust, you must use the same subnet as a tunnel interface with an IP address and netmask, or in the same subnet as the IP address and netmask of an interface bound to a Layer 3 (L3) security zone.

- When defining a MIP an interface in the Untrust zone, you can use a different subnet than the Untrust zone interface IP address. However, you must add a route on the external router pointing to an Untrust zone interface so that incoming traffic can reach the MIP. You must also define a static route that associates the MIP with the interface that hosts it.

- On some security devices, you can assign a MIP the same address as an interface, but you cannot use that MIP address in a DIP pool.

You can use a MIP as the destination addresses in rules between any two zones or in a Global rule. For the destination zone, use either the Global zone or the zone with the address to which the MIP points.

**EXAMPLE: CONFIGURING A MIP ON THE UNTRUST INTERFACE**

In this example, you create a MIP to handle inbound traffic to your Web server. After configuring the MIP, you create a Global MIP to represent the MIP you created for the device, then use the Global MIP object in a Security Policy rule that permits HTTP traffic from any address in the Untrust zone to the MIP—and to the host with the address to which the MIP points—in the Trust zone. All security zones are in the trust-vr routing domain.
1. Add a NetScreen-50 security device. Choose Model when adding the device and configure the device as running ScreenOS 5.x.

2. Configure the Trust interface for ethernet1.
   a. In the device navigation tree, select Network > Interface.
   c. Configure the IP address as 10.1.1.1 and the Netmask as 24. Leave all other settings as default.
   d. Click OK to save your changes.

3. Configure the Untrust interface for ethernet2.
   a. In the device navigation tree, select Network > Interface.
   c. Configure the IP address as 1.1.1.1 and the Netmask as 24. Leave all other settings as default.
   d. Click OK to save your changes.

4. Configure the MIP for ethernet2:
   b. In the interface navigation tree, select NAT > MIP to display the MIP screen.
c. Click the Add icon and configure the following:

- For Mapped IP, enter 1.1.1.5
- For Netmask, enter 32.
- For Host IP, enter 10.1.1.5
- For virtual router, select trust-vr

d. Click OK to save the MIP.

5. Click OK to save your changes to the interface, then click OK to save your changes to the device.

6. Create a Global MIP to reference the MIP you created for the device. You use a Global MIP when configuring NAT in a Security Policy rule; the Global MIP references the MIP for an individual device, enabling you to use one object (the Global MIP object) to represent multiple MIPs in a single rule.

a. In the navigation tree, select Object Manager > NAT Objects > MIP.

b. Click the Add icon to display the new Global MIP dialog box.

c. Configure the Global MIP as shown below:

   Figure 51: Configure Global MIP

7. Configure a firewall rule to route inbound HTTP traffic to the MIP address, as shown below:
Configuring VIPs

A virtual IP (VIP) address maps traffic received at one IP address to another address based on the destination port number in the TCP or UDP segment header. The destination IP addresses are the same, and the destination port numbers determine the host to which the traffic is sent. The security device forwards incoming traffic destined for a VIP to the host with the address to which the VIP points. When a VIP host initiates outbound traffic, the security device translates the source IP address of the host to that of the VIP address.

You can set a VIP only on an interface in the Untrust zone, and you must assign the VIP an IP address that is in the same subnet as an interface in the Untrust zone. Some security devices also support:

- Assigning the VIP the exact same address as the interface.
- Assigning the VIP to a dynamic IP address. When using a VIP with an interface in the Untrust zone that receives its IP address dynamically via DHCP or PPPoE, select the Same as the untrusted interface IP address option when setting up the VIP.

Additionally, the host to which the security device maps VIP traffic must be reachable from the trust-vr. If the host is in a routing domain other than that of the trust-vr, you must define a route to reach it.

You can use a VIP as the destination addresses in rules between any two zones or in a Global rule. For the destination zone, use either the Global zone or the zone with the address to which the VIP points.

Mapping Services and Ports

You can use virtual port numbers for well-known services when running multiple server processes on a single machine. For example, you can run two FTP servers on the same machine, one server on port 21 and the other on port 2121. Only users who know the virtual port number can append it to the IP address in the packet header to gain access to the second FTP server.

You can map predefined and custom services in a VIP. A single VIP can support custom services with:

- The same source and destination port numbers but different transports.
- Single port entries (by default).
- Multiple port entries, when you creating multiple service entries under a VIP (one service entry in the VIP for each port entry in the service).
Any destination port number or number range from 1 to 65,535, not just from 1024 to 65,535.

**EXAMPLE: CONFIGURING A VIP**

In this example, you create a VIP to handle inbound traffic to your Web server. After configuring the VIP, you create a Global VIP to represent the VIP you created for the device, then use the Global VIP object in a Security Policy rule that permits HTTP traffic on port 80 from any address in the Untrust zone to the MIP—and to the host with the address and port to which the MIP points—in the Trust zone. All security zones are in the trust-vr routing domain.

Because the VIP is in the same subnet as the Untrust zone interface, you do not need to define a route for traffic from the Untrust zone to reach it. (To route HTTP traffic from a security zone other than the Untrust zone to the VIP, you must set a route for 1.1.1.10 on the router in the other zone to point to an interface bound to that zone.)

Figure 53: Configure VIP Example Overview

1. **Add a NetScreen-204 security device.** Choose Model when adding the device and configure the device as running ScreenOS 5.x.

2. **Configure the Trust interface for ethernet1.**
   
   a. In the device navigation tree, select Network > Interface.
   
   
   c. Configure the IP address as 10.1.1.1 and the Netmask as 24. Leave all other settings as default.
   
   d. Click OK to save your changes.

3. **Configure the Untrust interface for ethernet3.**
   
   a. In the device navigation tree, select Network > Interface.
   
   
   c. Configure the IP address as 1.1.1.1 and the Netmask as 24. Leave all other settings as default.
d. Click OK to save your changes.

4. Configure the VIP for ethernet3:
   b. In the interface navigation tree, select NAT > VIP to display the VIP screen.
   c. Click the Add icon to display the Virtual IP dialog box. Enter the Virtual IP as 1.1.1.10.
   d. Click the Add icon to display the VIP mapping dialog box. Configure the following:
      - For Virtual Port, enter 80.
      - For Mapped IP, 10.1.1.10.
      - For Mapped Service, enter HTTP.
   e. Click OK to save the VIP mapping, then click OK to save the VIP.

5. Click OK to save your changes to the interface, then click OK to save your changes to the device.

6. Create a Global VIP to reference the VIP you created for the device. You use a Global VIP when configuring NAT in a firewall rule; the Global VIP references the VIP for the individual device, enabling you to use one object (the Global VIP object) to represent multiple VIPs in a single rule.
   a. In the navigation tree, select Object Manager > NAT Objects > VIP.
   b. Click the Add icon to display the new Global VIP dialog box.
   c. Configure the Global VIP as shown below:
7. Configure a firewall rule to route inbound HTTP traffic on port 80 to the VIP address, as shown below:

**Figure 55: Configure a Firewall Rule to Use a Global VIP**

<table>
<thead>
<tr>
<th>From Zone</th>
<th>Source</th>
<th>To Zone</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>untrust</td>
<td>any</td>
<td>trust</td>
<td>Web VIP</td>
<td>HTTP</td>
<td>permit</td>
<td>NS-204</td>
</tr>
</tbody>
</table>

**Configuring DIPs**

A dynamic IP (DIP) pool is a range of IP addresses. The security device can dynamically or deterministically use these IP addresses when performing network address translation on the source IP address (NAT-src) in IP packet headers.

- If the range of addresses in a DIP pool is in the same subnet as the interface IP address, the pool must exclude the interface IP address, router IP addresses, and any mapped IP (MIP) or virtual IP (VIP) addresses that might also be in that subnet.

- If the range of addresses is in the subnet of an extended interface, the pool must exclude the extended interface IP address.

You can assign DIP pools to physical interfaces and subinterfaces for network and VPN traffic, and tunnel interfaces for VPN tunnels only.
Port Address Translation

Use Port Address Translation (PAT) to enable multiple hosts (up to 64,500) to share the same IP address. The security device maintains a list of assigned port numbers to distinguish which session belongs to which host. Use PAT in conjunction with a MIP and a DIP pool to resolve the problem of overlapping address spaces.

Some applications, such as NetBIOS Extended User Interface (NetBEUI) and Windows Internet Naming Service (WINS), require specific port numbers and do not work with PAT. For these applications, you cannot use PAT; you must configure the DIP pool to use a fixed port (numbered IP). For fixed-port DIP, the security device hashes and saves the original host IP address in its host hash table, enabling the device to associate the right session with each host.

EXAMPLE: CREATING A DIP POOL WITH PORT ADDRESS TRANSLATION (PAT)

In this example, you want to create a VPN tunnel for users at one site to reach an FTP server at another site. However, the internal networks at both sites use the same private address space of 10.1.1.0/24.

On the first device, an NetScreen-HSC, you create a tunnel interface in the Untrust zone with IP address 10.10.1.1/24, and associate it with a DIP pool containing the IP address range 10.10.1.2–10.10.1.2 (addresses in the neutral address space of 10.10.1.0/24). You enable port address translation for the DIP pool. On the second device, an NetScreen-208, you create a tunnel interface with an IP address in a neutral address space and set up a Mapped IP (MIP) address to its FTP server. This example provides details on configuring the NetScreen-HSC to use a DIP pool with PAT; details on configuring the second device in the VPN are not provided.

1. Add a NetScreen-HSC security device. Choose Model when adding the device and configure the device as running ScreenOS 5.x.

2. Configure the tunnel interface:

   a. In the device navigation tree, select Network > Interface.

   b. Click the Add icon and select New > Tunnel Interface. The General Properties screen appears.

   c. Configure the tunnel interface as shown below:
3. Configure the DIP pool:
   a. In the interface navigation tree, select NAT > DIP to display the DIP screen.
   b. Click the Add icon to display the DIP pool dialog box. Configure the following, then click OK:
      - For DIP ID, enter 5.
      - For Start, enter 10.10.1.2
      - For End, enter 10.10.1.2

4. Click OK to save your changes to the interface, then click OK to save your changes to the device.

DIP with Extended Interface
If circumstances require that the source IP address in outbound firewall traffic be translated to an address in a different subnet from that of the egress interface, you can use the extended interface option. This option enables you to graft a second IP address and an accompanying DIP pool onto an interface that is in a different subnet. You can then enable NAT on a per-policy basis and specify the DIP pool built on the extended interface for the translation.

EXAMPLE: USING DIP IN A DIFFERENT SUBNET
In this example, two branch offices have leased lines to a central office. The central office requires them to use only the authorized IP addresses it has assigned them. However, the offices receive different IP addresses from their ISPs for Internet traffic. For communication with the central office, you use the extended interface option to configure the security device in each branch office to translate the source IP address in packets it sends to the central office to the authorized address. The authorized and assigned IP addresses for branch offices A and B are as follows:
Table 13: Assigned IP Addresses for Office A and Office B

<table>
<thead>
<tr>
<th></th>
<th>Assigned IP Address (from ISP) Used for Untrust Zone Physical Interface</th>
<th>Authorized IP Address (from Central Office) Used for Untrust Zone Extended Interface DIP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office A</td>
<td>195.1.1.1/24</td>
<td>211.10.1.1/24</td>
</tr>
<tr>
<td>Office B</td>
<td>201.1.1.1/24</td>
<td>211.20.1.1/24</td>
</tr>
</tbody>
</table>

The security devices at both sites have a Trust zone and an Untrust zone. All security zones are in the trust-vr routing domain. You bind ethernet1 to the Trust zone and assign it IP address 10.1.1.1/24. You bind ethernet3 to the Untrust zone and give it the IP address assigned by the ISPs: 195.1.1.1/24 for Office A and 201.1.1.1/24 for Office B. You then create an extended interface with a DIP pool containing the authorized IP address on ethernet3:

- Office A—extended interface IP 211.10.1.10/24; DIP pool 211.10.1.1 – 211.10.1.1; PAT enabled
- Office B—extended interface IP 211.20.1.10/24; DIP pool 211.20.1.1 – 211.20.1.1; PAT enabled

You set the Trust zone interface in NAT mode. It uses the Untrust zone interface IP address as its source address in all outbound traffic except for traffic sent to the central office. You configure a policy to the central office that translates the source address to an address in the DIP pool in the extended interface. (The DIP pool ID number is 5. It contains one IP address, which, with port address translation, can handle sessions for ~ 64,500 hosts.) The MIP address that the central office uses for inbound traffic is 200.1.1.1, which you enter as “HQ” in the Untrust zone address book on each security device.

Each ISP must set up a route for traffic destined to a site at the end of a leased line to use that leased line. The ISPs route any other traffic they receive from a local security device to the Internet.

Figure 57: Using DIP in Different Subnets Example Overview

Note: Leased lines connect branch offices A and B directly to the central office.
1. Add the devices:
   a. For Office A, add a NetScreen-208 security device.
   b. For Office B, add a NetScreen-204 security device.

2. Configure ethernet1 (Trust Zone) for Office A:
   a. Double-click Office A device to open the device configuration. In the device navigation tree, select Network > Interface.
   c. Configure IP address/netmask as 10.1.1.1/24 and Interface Mode as NAT.
   d. Click OK to save your changes.

3. Configure ethernet3 (Untrust Zone) for Office A:
   a. In the device navigation tree, select Network > Interface.
   c. Configure IP address/netmask as 195.1.1.1/24 and Interface Mode as Route.
   d. In the interface navigation tree, select NAT > DIP. Click the Add icon to display the DIP pool dialog box. Configure the DIP as shown below, then click OK:
      - For Start, enter 211.10.1.1.
      - For End, enter 211.10.1.1.
      - For Extended IP, enter 211.10.1.10.
      - For Netmask, enter 24.

4. Add the route to the Corporate Office on the trust-vr of Office A:
   a. In the device navigation tree, select Network > Routing. Double-click the trust-vr router. The General Properties screen appears.
   b. In the trust-vr navigation tree, select Routing Table. Click the Add icon and configure the new route:
      - Set the IP address/netmask to 0.0.0.0/0.
      - For Next Hop, select Gateway; the gateway options appear.
      - For Interface, select ethernet3.
      - For Gateway IP Address, enter 195.1.1.254.
      Leave all other defaults, then click OK to save the route.
c. Click OK to save your changes to the trust-vr, then click OK to save your changes and close the Office A device configuration.

5. Configure ethernet1 (Trust Zone) for Office B:
   a. Double-click Office B device to open the device configuration. In the device navigation tree, select Network > Interface.
   c. Configure IP address/netmask as 10.1.1.1/24 and Interface Mode as NAT.
   d. Click OK to save your changes.

6. Configure ethernet3 (Untrust Zone) for Office B:
   a. In the device navigation tree, select Network > Interface.
   c. Configure IP address/netmask as 201.1.1.1/24 and Interface Mode as Route.
   d. In the interface navigation tree, select NAT > DIP. Click the Add icon to display the DIP pool dialog box. Configure the DIP as shown below, then click OK:
      - For Start, enter 211.20.1.1.
      - For End, enter 211.20.1.1.
      - For Extended IP, enter 211.20.1.10.
      - For Netmask, enter 24.

7. Add the route to the Corporate Office on the trust-vr of Office B:
   a. In the device navigation tree, select Network > Routing. Double-click the trust-vr router. The General Properties screen appears.
   b. In the trust-vr navigation tree, select Routing Table. Click the Add icon and configure the new route:
      - Set the IP address/netmask to 0.0.0.0/0.
      - For Next Hop, select Gateway; the gateway options appear.
      - For Interface, select ethernet3.
      - For Gateway IP Address, enter 201.1.1.254.
      - Leave all other defaults, then click OK to save the route.
   c. Click OK to save your changes to the trust-vr, then click OK to save your changes and close the Office A device configuration.
8. Add the Address Object that represents HQ:
   a. In the main navigation tree, select Object Manager > Address Objects. Click the Add icon and select Host. The New Host dialog box appears.
   b. Configure the Host as detailed below, then click OK:
      - For Name, enter Central Office HQ.
      - Select IP, then enter the IP Address 200.1.1.1.

9. Create a Global DIP to reference the DIP pool on each device. You use a Global DIP when configuring NAT in a firewall rule; the Global DIP references the DIP pool for an individual device, enabling you to use one object (the Global DIP object) to represent multiple DIP pools in a single rule.
   a. In the navigation tree, select Object Manager > NAT Objects > DIP.
   b. Click the Add icon to display the new Global DIP dialog box. Configure the Global DIP as shown below, then click OK:

   ![Global DIP Configuration](image)

   ![Office A and Office B DIPs](image)
10. Configure two firewall rules, one which uses the Global DIP object for NAT translation, as shown below:

**Figure 59: Configure Two Firewall Rules to Use Global DIP**

<table>
<thead>
<tr>
<th>Match</th>
<th>Action</th>
<th>Install On</th>
<th>Rule Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>trust</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>any</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>trust</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>any</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Incoming DIP for SIP Traffic**

Use an Incoming DIP to enable the managed device to handle incoming Session Initiation Protocol (SIP) calls. SIP is an Internet Engineering Task Force (IETF)-standard protocol for initiating, modifying, and terminating multimedia sessions (such as conferencing, telephony, or multimedia) over the Internet. SIP is used to distribute the session description, to negotiate and modify the parameters of an existing session, and to terminate a multimedia session.

**NOTE:** SIP is a predefined service that uses port 5060 as the destination port. To specify the SIP service in the Service column of a firewall rule, you must select the predefined service group VOIP, which includes the H.323 and SIP service objects.

To use SIP, a caller must register with the registrar before SIP proxies and location servers can identify where the caller wants to be contacted. A caller can register one or more contact locations by sending a REGISTER message to the registrar. The REGISTER message contains the address-of-record URI and one or more contact URIs. When the registrar receives the message, it creates bindings in a location service that associates the address-of-record with the contact addresses.

The security device monitors outgoing REGISTER messages from SIP users, performs NAT on these addresses, and stores the information in an Incoming DIP table. When the device receives an INVITE message from the external network, it uses the Incoming DIP table to identify which internal host to route the INVITE message to.
To enable the device to perform NAT on incoming SIP calls, you must configure an interface DIP or DIP pool on the egress interface of the device. A single interface DIP is adequate for handling incoming calls in a small office; a DIP pool is recommended for larger networks or an enterprise environment.

**NOTE:** SIP uses UDP as its transport protocol. When using your managed device to handle SIP traffic, you might also want to enable UDP Flood Protection. For details on configuring UDP Flood Protection, see “Configuring UDP Flooding Protection” on page 223.

**EXAMPLE: CONFIGURING AN INTERFACE DIP FOR SIP**

In this example, you configure an interface-based DIP on the Untrust interface of the security device, then configure a firewall rule that permits SIP traffic from the Untrust zone to the Trust zone and references the interface DIP. You also configure a rule that permits SIP traffic from the Trust to the Untrust zone using NAT Source, which enables hosts in the Trust zone to register with the proxy in the Untrust zone.

1. Add a NetScreen-208 device named Office A. Choose Model when adding each device and configure as running ScreenOS 5.1.

2. Configure ethernet1 (Trust Zone) for Office A:
   a. Double-click Office A device to open the device configuration. In the device navigation tree, select Network > Interface.
   c. Configure IP address/netmask as 10.1.1.1/24 and Interface Mode as NAT.
   d. Click OK to save your changes.

3. Configure ethernet3 (Untrust Zone) for Office A:
   b. Configure IP address/netmask as 1.1.1.1/24.
   c. In the interface navigation tree, select NAT > DIP, then click the Interface DIP tab.
d. Select Incoming NAT.

e. Click OK to save your changes to the interface, then click OK again to save your changes to the device.

4. Create a Global DIP to reference the Interface DIP on Office A. You use a Global DIP when configuring NAT in a firewall rule; the Global DIP references the Interface DIP for an individual device.

a. In the navigation tree, select Object Manager > NAT Objects > DIP.

b. Click the Add icon to display the new Global DIP dialog box.

c. Configure the Global DIP as shown below:

Figure 61: Configure Global DIP for Interface DIP

5. Configure firewall rules:

- Rule 1 handles outgoing SIP traffic, and uses the outgoing interface to perform NAT.

- Rule 2 handles incoming SIP traffic, and uses the Interface DIP as the Destination to perform NAT.

Both rules are shown below:
EXAMPLE: CONFIGURING AN INCOMING DIP POOL FOR SIP

In this example, you configure a DIP pool on the Untrust interface to perform NAT on incoming SIP calls. After creating the DIP pool and Global DIP object, you configure a firewall rule to permit SIP traffic from the Untrust zone to the Trust zone and reference the DIP pool. You also configure a rule to permit SIP traffic from the Trust to the Untrust zone, which enables hosts in the Trust zone to register with the proxy in the Untrust zone.

1. Add a NetScreen-204 device named Office B. Choose Model when adding each device and configure as running ScreenOS 5.1.
2. Configure ethernet1 (Trust Zone) for Office B:
   a. Double-click Office B device to open the device configuration. In the device navigation tree, select Network > Interface.
   c. Configure IP address/netmask as 10.1.1.1/24 and Interface Mode as NAT.
   d. Click OK to save your changes.

3. Configure ethernet3 (Untrust Zone) for Office B:
   b. Configure IP address/netmask as 1.1.1.1/24.
   c. In the interface navigation tree, select NAT > DIP, then click the Add icon. The new DIP Pool dialog box appears. Configure as detailed below, then click OK:
      - For ID, enter 4.
      - For Start, enter 1.1.1.20.
      - For End, enter 1.1.1.40.
      - Select Incoming NAT.
   d. Click OK again to save your changes to the device.

4. Create a Global DIP to reference the Incoming NAT DIP on Office B. You use a Global DIP when configuring NAT in a firewall rule; the Global DIP references the Incoming NAT DIP for an individual device.
   a. In the navigation tree, select Object Manager > NAT Objects > DIP.
   b. Click the Add icon to display the new Global DIP dialog box.
   c. Configure the Global DIP as shown below:
5. Configure firewall rules:

- Rule 1 handles outgoing SIP traffic, and uses the outgoing interface to perform NAT.

- Rule 2 handles incoming SIP traffic, and uses the Interface DIP to perform NAT.

Both rules are shown below:


**Interface Configuration Examples**

The following sections detail each interface type and provide configuration examples.

**Configuring an Aggregate Interface**

An aggregate interface combines two or more physical interfaces, enabling each member to share equally the traffic load on the aggregate interface IP address. Use an aggregate interface to increase the amount of bandwidth available to a single IP address. You can also provide redundancy: If one member of an aggregate interface fails, the other members can continue processing traffic—although with less bandwidth than previously available.

The NetScreen-5000 series supports aggregate interfaces with Secure Port Modules (SPMs):

- The 5000-8G SPM supports up to four aggregate interfaces.
- The 5000-24FE SPM supports up to five aggregate interfaces.

You must assign one of the following names to the aggregate interface: aggregate1, aggregate2, aggregate3, aggregate4, or aggregate5.

**EXAMPLE: CONFIGURING AN AGGREGATE INTERFACE**

In this example, you combine two Gigabit Ethernet mini-GBIC ports, each running at 1 Gbps, into an aggregate interface (aggregate1) running at 2-Gbps. The aggregate interface combines Ethernet ports 1 and 2 on a 5000-8G SPM (residing in Slot 2) and is bound to the Trust zone.

1. Add a NetScreen-5200 device running ScreenOS 5.x, then configure the network module:
   a. Double-click the device icon to open the device configuration. In the device navigation tree, select Network > Slot.
   b. Double-click slot 2 to display the slot configuration dialog box. For Card Type, select 5000-8G SPM.
   c. Click OK to save the slot configuration.

2. Configure the aggregate interface:
   a. In the device navigation tree, select Network > Interface.
   b. Click the Add icon and select Aggregate Interface. The General Properties screen appears.
   c. Configure the following:
      - For Zone, select Trust.
      - For IP address/netmask, enter 10.1.1.0/24.
      - For Interface Mode, ensure that the mode is set to NAT.
d. Click OK to save your changes.

3. Add the ethernet 2/1 interface as a member of the aggregate1 interface.
   b. Configure the Parent Aggregate Interface as aggregate1.
   c. Click OK to save your changes.

4. Add the ethernet 2/2 interface as a member of the aggregate1 interface.
   b. Configure the Parent Aggregate Interface as aggregate1.
   c. Click OK to save your changes.

5. Click OK to save your changes to the device.

Configuring a Multilink Interface

On an SSG 520/550 security device, you configure and access multiple serial links called a bundle, through a virtual interface called a multilink interface. The multilink interface emulates a physical interface for the transport of frames.

EXAMPLE: CONFIGURING A MULTILINK INTERFACE
In this example, you combine two WAN subinterfaces into an multilink interface. The name of the multilink interface must be mlid_num. For example, multilink interface names can be ml1, ml2, and so on.

1. Add an SSG 520 (or SSG 550) device running ScreenOS 5.1SSG, then configure the network module:
   a. Double-click the device icon to open the device configuration. In the device navigation tree, select Network > Slot.
   b. Double-click slot 2 to display the slot configuration dialog box. For Card Type, select .
   c. Click OK to save the slot configuration.

2. Configure the multilink interface:
   a. In the device navigation tree, select Network > Interface.
   b. Click the Add icon and select Multilink Interface. The General Properties screen appears.
   c. Configure the following:
      - For Name, accept the default
For Zone, select Trust

For Encapsulation Type, select mlfr-uni-nni

d. Configure MLFR options:
   - For Name, accept the default
   - For Zone, select Trust

e. Click OK to save your changes.

3. Click OK to save your changes to the device.

Configuring a Loopback Interface

A loopback interface emulates a physical interface on a security device. However, unlike a physical interface, a loopback interface is always in the up state as long as the device on which it resides is up. You might want to use a loopback interface as:

- The management interface—You can manage the device using either the IP address of a loopback interface or the manage IP address that you assign to a loopback interface.

- A Virtual Security Interface (VSI) for NSRP—The physical state of the VSI on the loopback interface is always up. The interface can be active or not, depending upon the state of the VSD group to which the interface belongs.

- A source interface for specific traffic (such as syslog packets) that originates from the device—When you define a source interface for an application, the specified source interface address is used instead of the outbound interface address to communicate with an external device.

Loopback interfaces are named loopback.id_num, where id_num is a number greater than or equal to 1 (the maximum id_num value you can specify is platform-specific) and denotes a unique loopback interface on the device. Like a physical interface, you must assign an IP address to a loopback interface and bind it to a security zone.

NOTE: You cannot bind a loopback interface to a HA zone, nor can you configure a loopback interface for layer 2 operation or as a redundant/aggregate interface. You cannot configure the following features on loopback interfaces: NTP, DNS, VIP, secondary IP, track IP, or Webauth.

After defining a loopback interface, you can then define other interfaces as members of its group. Traffic can reach a loopback interface if it arrives through one of the interfaces in its group. Any interface type can be a member of a loopback interface group—physical interface, subinterface, tunnel interface, redundant interface, or VSI.

EXAMPLE: CONFIGURING A LOOPBACK INTERFACE

In this example, you create the loopback interface loopback.1, bind it to the Untrust zone, and assign the IP address 1.1.1.27/24 to it.
Chapter 5: Configuring Devices

1. Add a device.

2. Configure the loopback interface:
   a. In the device navigation tree, select Network > Interface.
   b. Click the Add icon and select Loopback Interface. The General Properties screen appears.
   c. Configure the following:
      - For zone, select Untrust.
      - For IP Address/Netmask, enter 1.1.1.27/24
      - Ensure that Manageable is enabled.
      - Ensure that the Management IP is 1.1.1.27.
   d. Click OK to save the new interface.

3. Click OK to save your changes to the device.

Configuring Virtual Security Interfaces (VSIs)

Virtual security interfaces (VSIs) are the virtual interfaces that two security devices forming a virtual security device (VSD) share when operating in high availability (HA) mode. Network and VPN traffic use the IP address and virtual MAC address of a VSI. The VSD then maps the traffic to the physical interface, subinterface, or redundant interface to which you have previously bound the VSI. When two security devices are operating in HA mode, you must bind security zone interfaces that you want to provide uninterrupted service in the event of a device failover to one or more virtual security devices (VSDs). When you bind an interface to a VSD, the result is a virtual security interface (VSI).

For more details and an example on configuring VSIs, see “Configuring NSRP Clusters” on page 379.

Configuring a Redundant Interface

A redundant interface combines two physical interfaces to create one redundant interface, which you can then bind to a security zone. One of the two physical interfaces acts is the primary interface and handles all the traffic directed to the redundant interface; the other physical interface is the secondary interface and stands by. If the primary interface fails, traffic to the redundant interface fails over to the secondary interface, which becomes the new primary interface.
Because redundant interfaces enable failover at the interface level, before a failure escalates to the device failover level, they are often used when deploying two security devices in a High Availability configuration. You can use the dedicated physical redundant HA interfaces or bind two generic interfaces to the HA zone (you can also create redundant security zone interfaces). Then, if the link from the primary interface to the switch becomes disconnected, the link fails over to the secondary interface, preventing a device failover from the VSD master to backup.

**NOTE:** You cannot combine subinterfaces in a redundant interface. However, you can define a VLAN on a redundant interface in the same way that you can define a VLAN on a subinterface.

**EXEMPLARY: CONFIGURING REDUNDANT INTERFACES FOR VSI GROUPS**

In this example, devices A and B are members of two VSD groups—VSD group 0 and VSD group 1—in an active/active configuration. Device A is the master of VSD group 0 and the backup in VSD group 1. Device B is the master of VSD group 1 and the backup in VSD group 0. The devices are linked to two pairs of redundant switches—switches A and B in the Untrust zone, and switches C and D in the Trust zone.

Because devices A and B are members of the same NSRP cluster, device A propagates all interface configurations to device B except the manage IP address, which you enter on the redundant2 interface on both devices. You put ethernet1/1 and ethernet1/2 in redundant1, and ethernet2/1 and ethernet2/2 in redundant2. On the redundant2 interface, you define a manage IP of 10.1.1.21 for device A and a manage IP of 10.1.1.22 for device B on this interface.

The physical interfaces that are bound to the same redundant interface connect to different switches:

- Physical interfaces bound to a redundant interface in the Untrust zone:
  - ethernet1/1 to switch A, ethernet1/2 to switch B
- Physical interfaces bound to a redundant interface in the Trust zone:
  - ethernet2/1 to switch C, ethernet2/2 to switch D.

By putting ethernet1/1 and ethernet2/1 in their respective redundant interfaces first, you designate them as primary interfaces. If the link to a primary interface becomes disconnected, the device reroutes traffic through the secondary interface to the other switch without requiring the VSD master device to fail over.

The physical interfaces do not have to be in the same security zone as the redundant interface to which you bind them. IP addresses for multiple VSIs can be in the same subnet or in different subnets if the VSIs are on the same redundant interface, physical interface, or subinterface. If the VSIs are on different interfaces, they must be in different subnets. The IP addresses for the VSIs:

<table>
<thead>
<tr>
<th>Table 14: IP Addresses for VSIs</th>
</tr>
</thead>
<tbody>
<tr>
<td>VSIs for VSD Group 0</td>
</tr>
<tr>
<td>----------------------</td>
</tr>
<tr>
<td>redundant1</td>
</tr>
<tr>
<td>redundant2</td>
</tr>
</tbody>
</table>
In this example, if the cable from ethernet1/1 becomes disconnected, the port fails over to ethernet1/2. Consequently, all the traffic to and from devices A and B passes through switch B. Reconnecting the cable from ethernet1/1 on device A to switch A automatically causes that interface to regain its former priority.

Figure 66: Redundant Interfaces for VSIs

1. Add the cluster and member devices:
   a. For the cluster, specify NetScreen-500 security devices running ScreenOS 5.1.
   b. Add member Device A.
   c. Add member Device B.

2. Create a new VSD definition for the cluster:
   a. Double-click the Office 1 Cluster to open the cluster configuration.
   b. In the cluster navigation tree, select Members.
   c. In the VSD Definitions area, click the Add icon.
   d. Enter 2, then click OK to save the new VSD definition.

3. Configure the cluster network module (slot1):
   a. In the cluster navigation tree, select Network > Slot.
   b. Double-click slot 1 to display the slot configuration dialog box. For Card Type, select 2 Interfaces (10/100).
c. Click OK to save the slot configuration. Repeat process to add a new network module for slot 2.

4. Configure the redundant1 interface:
   a. In the cluster navigation tree, select Network > Interface.
   b. Click the Add icon and select Redundant Interface. The General Properties screen appears.
   c. Configure the following, then click OK:
      - For Zone, select Untrust.
      - For IP address/netmask, enter 210.1.1.1/24.
      - Ensure that Manageable is enabled.
      - Ensure that the Management IP is 210.1.1.1.

5. Add ethernet1/1 as a member of the redundant1 interface:
   b. Configure the Redundant Interface Group as redundant1, then click OK to save your changes.

6. Add ethernet1/2 as a member of the redundant1 interface:
   b. Configure the Redundant Interface Group as redundant1, then click OK to save your changes.

7. Configure the redundant2 interface:
   a. In the cluster navigation tree, select Network > Interface.
   b. Click the Add icon and select Redundant Interface. The General Properties screen appears.
   c. Configure the following, then click OK:
      - For Zone, select Trust.
      - For IP address/netmask, enter 10.1.1.1/24.

8. Add ethernet2/1 as a member of the redundant2 interface:
   b. For Redundant Interface Group, select redundant2.
c. Click OK to save your changes.

9. Add ethernet2/2 as a member of the redundant2 interface:
   b. For Redundant Interface Group, select redundant2.
   c. Click OK to save your changes.

10. Add the VSI interface for redundant1:
    a. In the cluster navigation tree, select Network > Interfaces. Click the Add icon and select VSI. The General Properties screen appears.
    b. Configure the following, then click OK:
       - For Name, select redundant 1, then select 1 (for VSD Group 1).
       - For IP address/Netmask, enter 210.1.1.2/24.
       - Ensure that Manageable is enabled.

11. Add the VSI interface for redundant2:
    a. In the cluster navigation tree, select Network > Interfaces. Click the Add icon and select VSI. The General Properties screen appears.
    b. Configure the following, then click OK:
       - For Name, select redundant 2, then select 1 (for VSD Group 1).
       - For IP address/Netmask, enter 10.1.1.2/24.
       - Ensure that Manageable is enabled.

12. Click Apply to apply your changes to the cluster and propagate the settings to each member device.

13. Configure the Manage IP address for each member device:
    a. In the cluster navigation tree, select Members, then double-click Device A.
    b. In the device navigation tree, select Network > Interfaces, then double-click redundant2. The General Properties screen appears.
    c. For Management IP, enter 10.1.1.21, then click OK to save your changes.
    d. In the cluster navigation tree, select Members, then double-click Device B.
    e. In the device navigation tree, select Network > Interfaces, then double-click redundant2. The General Properties screen appears.
    f. For Management IP, enter 10.1.1.22, then click OK to save your changes.
14. Click OK to save your changes to the cluster.

Configuring a Subinterface

A subinterface, like a physical interface, is a doorway through which traffic enters and exits a security zone. You can logically divide a physical interface into several virtual subinterfaces, each of which borrows the bandwidth it needs from the physical interface. Subinterfaces use names that indicate their physical interface, such as ethernet3/2.1 or ethernet2.1.

You can create three types of subinterfaces:

- **None (For ScreenOS 5.0 devices only)**—The subinterface does not use VLAN tagging.
- **Tagged interface (VLAN)**—Using VLAN tagging, the subinterface distinguishes between traffic bound for it from traffic bound for other interfaces. For details on configuring VLAN tagging, see “Using VLAN IDs” on page 357.
- **Encapsulated (For ScreenOS 5.1 and higher devices only)**—Using encapsulation, you can create a PPPoE subinterface that does not use VLAN tagging. PPPoE subinterfaces enable the device to handle multiple PPPoE sessions over one physical interface.

**NOTE:** The number of PPPoE sessions per physical interface is determined by the security device platform. For details on configuring multiple PPPoE instances on one interface, see “Configuring PPPoE” on page 282.

You can create a subinterface on any physical interface in the root system or virtual system, and you can bind a subinterface to the same zone as its physical interface or to a different zone. However, the IP address of a subinterface must be in a different subnet from the IP addresses of all other physical interfaces and subinterfaces.

**EXAMPLE: CONFIGURING A SUBINTERFACE IN THE ROOT SYSTEM**

In this example, you create a subinterface for the Trust zone in the root system. You configure the subinterface on ethernet1, which is bound to the Trust zone. You bind the subinterface to a user-defined zone named “accounting”, which is in the trust-vr. You assign it subinterface ID 3, IP address 10.2.1.1/24, and VLAN tag ID 3. The interface mode is NAT.

1. Add a device.

2. Configure a new zone:
   a. Double-click the device icon to open the device configuration. In the device navigation tree, select Network > Zone.
   b. Click the Add icon and select Security Zone. The General Properties Screen appears.
   c. Configure the following, then click OK:
      - For Name, enter accounting.
3. Configure the Subinterface:
   a. In the device navigation tree, select Network > Interface.
   b. Click the Add icon and select Sub Interface. The General Properties screen appears.
   c. Configure the following, then click OK:
      - For Name, select ethernet1, then select 3.
      - For VLAN tag, enter 3.
      - For Zone, select accounting.
      - For IP Address/Netmask, enter 10.2.1.1/24
      - Ensure that Manageability is enabled.
      - Ensure that the Management IP is 10.2.1.1.
      - For Interface Mode, select NAT.
   4. Click OK to save your changes to the device.

Configuring a WAN Subinterface

Multilink Frame Relay (MLFR) for User-to-Network Interface (UNI) on SSG 520/550 security devices allow for the creation of one or more permanent virtual circuits (PVCs) within the bundle. You create a PVC by configuring a subinterface to the multilink interface. Each subinterface maps to a PVC, which is identified by a data-link connection identifier (DLCI). Note that each PVC can be associated with a separate security zone; the security zone for each PVC can be different from the security zone assigned to the multilink interface.

EXAMPLE: CONFIGURING A WAN SUBINTERFACE

In this example, you create a subinterface for the multilink interface and assign it to a security zone. Then assign a Frame Relay DLCI and IP address to the subinterface.

1. On an SSG 520 (or SSG 550) device running ScreenOS 5.1SSG, add a multilink interface and assign it to the Trust zone.

2. Add and configure a WAN-Sub Interface:
   a. In the device navigation tree, select Network > Interface.
   b. Click the Add icon and select WAN-Sub Interface. The General Properties screen appears.
   c. Configure the following, then click OK:
For Name, select the multilink interface that you want to assign the subinterface to. The subinterface name consists of the multilink interface name and a subinterface number. For example, if the multilink interface name is ml1, its subinterfaces can be ml1.1 and ml1.2.

For Zone, select Trust.

3. Click OK to save your changes to the device.

Configuring a Tunnel Interface

A tunnel interface is a doorway to a VPN tunnel. VPN traffic enters and exits a VPN tunnel via a tunnel interface. When you bind a tunnel interface to a VPN tunnel, you can use that tunnel interface to route VPN traffic to a specific destination.

NOTE: VPN Manager automatically creates the necessary tunnel interfaces for route-based VPNs. For device-level VPNs, you can create the tunnel interfaces before or after creating the VPN.

When creating a route-based VPN, you must create a tunnel interface to enable the security device to route traffic VPN traffic. You can bind a route-based VPN tunnel to a tunnel interface that is either numbered (with IP address/netmask) or unnumbered (without IP address/netmask).

Using Numbered Tunnel Interfaces

When the tunnel interface is numbered, you must give the interface an IP address and bind the tunnel interface to a tunnel zone. Using numbered tunnel interfaces enables you to use NAT services for policy-based VPN tunnels. Assign an IP address to a tunnel interface if you want the interface to support one or more dynamic IP (DIP) pools for source address translation (NAT-src) and mapped IP (MIP) addresses for destination address translation (NAT-dst).

You can create a numbered tunnel interface in a security zone or a tunnel zone.

Using Unnumbered Tunnel Interfaces

When the tunnel interface is unnumbered, you must specify the interface from which the tunnel interface borrows an IP address. The security device uses the borrowed IP address as a source address when the device itself initiates traffic—such as OSPF messages—through the tunnel. Use unnumbered tunnel interfaces when the tunnel interface does not need to support NAT services, and your configuration does not require the tunnel interface to be bound to a tunnel zone.

You can create an unnumbered tunnel interface that borrows the IP address from an interface in the same security zone or from an interface in a different zone, as long as both zones are in the same routing domain. However, you cannot bind the tunnel interface to a tunnel zone.
Configuring Maximum Transmission Unit (MTU) Size

(This option is supported by some security devices.) As packets traverse different networks, a networking component sometimes needs to break a packet into smaller pieces (fragments) based upon the maximum transmission unit (MTU) of each network. The networking component for the destination network must then reassemble the received fragments into a packet. Because fragmentation and reassembly can impact network performance, you might want to fragment a packet destined for a VPN tunnel as it passes through the tunnel interface (before the packet is encrypted and/or encapsulated).

For devices running ScreenOS 5.1 and higher, you can define an MTU size that controls the size of packets sent through the tunnel. When the tunnel interface receives the packet, it breaks the packet into fragments based on the specified MTU size, encrypts and/or encapsulates each fragment, then sends the traffic through the tunnel. As these packets (fragments) pass through other networks, they might be small enough that networking components do not need to perform further fragmentation—which reduces the network load and can decrease the time it takes to send VPN traffic. The receiving networking component (security device or external device) must still reassemble the fragments as they exit the other end of the VPN tunnel.

To configure an MTU size for a tunnel interface, in the tunnel interface navigation tree, select Advanced Properties and enter a value for MTU Size. By default, the size is set to none (the interface does fragment packets entering a VPN tunnel). The acceptable range is 800 to 1500.
Configuring an ADSL Interface

Asymmetric Digital Subscriber Line (ADSL) is a Digital Subscriber Line (DSL) technology that enables existing telephone lines to carry both voice telephone service and high-speed digital transmission. To use ADSL with a security device, you must configure the adsl1 interface on the NetScreen-5GT ADSL security device (which supports ADSL).

About ADSL

Traditional telephone lines use analog signals to carry voice service through twisted-pair copper wires. However, when using analog transmission, the service provider can use only a small portion of the available bandwidth. To work around this limitation, the service provider can use digital transmission to access a wider bandwidth on the same media, at the same time. Because the service provider separates analog and digital transmissions, you can use your telephone and connect the Internet with your computer at the same time on the same line.

At the service provider’s central office, the Digital Subscriber Line Access Multiplexer (DSLAM) connects many DSL lines to a high-speed network such as an Asynchronous Transfer Mode (ATM) network. ADSL transmission is asymmetric because the rate at which you can send data (the upstream rate) is considerably less than the rate at which you can receive data (the downstream rate). ADSL is ideal for Internet access because most messages sent to the Internet are small and do not require much upstream bandwidth, while most data received from the Internet require greater downstream bandwidth.

You can use the ADSL port on the NetScreen-5GT ADSL security device to enable Internet access for a network—without adding additional phone lines, and without using an additional ADSL modem. For details on connecting and cabling the NetScreen-5GT ADSL, see the NetScreen-5GT ADSL User’s Guide.

About the ADSL Interface

The ADSL interface on the NetScreen-5GT ADSL security device uses ATM as its transport layer. The interface supports multiple permanent virtual circuits (PVCs), which are continuously-available logical connections to the network, on a single physical line (the adsl1 interface). You can configure additional virtual circuits on the device by creating subinterfaces (such as adsl1.1, adsl1.2).

Before you can configure the adsl1 interface, however, you must obtain the DSLAM configuration details for the ADSL connection from the service provider, as detailed below.

ADSL Settings (Provided by the Service Provider)

The service provider for ADSL Internet access must provide you with some details about the ADSL connection so you can configure the security device to connect to their servers. Not all service providers use the same implementation of ADSL; you might be given any combination of the following ADSL parameters:

- Virtual Path Identifier and Virtual Channel Identifier (VPI/VCI), which identify the virtual circuit on the DSLAM.
ATM encapsulation method (Multiplexing mode). The ADSL interface on the security device supports the following ATM Adaptation Layer 5 (AAL5) encapsulations:

- Virtual Circuit (VC)-based multiplexing, in which each protocol is carried over a separate ATM virtual circuit.
- Logical Link Control (LLC), which enables several protocols to be carried on the same ATM virtual circuit (default encapsulation method). This is the default option for the ADSL1 interface on the NetScreen-5GTADSL security device.

The service provider must tell you the type of multiplexing used on the ADSL line.

Point-to-Point Protocol (PPP) is a standard protocol for transmitting IP packets over serial point-to-point links, such as an ATM PVC. The security device supports the following methods of transporting PPP packets:

- PPP over Ethernet (PPPoE). RFC 2516 describes the encapsulation of PPP packets over Ethernet. For more information about PPPoE, see “Configuring PPPoE” on page 282.
- PPP over AAL5 (PPPoA). RFC 1483 describes the encapsulation of network traffic over AAL5. For more information about PPPoA, see “Configuring PPPoA” on page 289.

If the service provider’s network uses PPPoE or PPPoA, the service provider must give you the user name and password for the connection, the authentication method used, and any other protocol-specific parameters.

IP addresses. The service provider might give the network a static IP address or a range of IP addresses. The service provider should also give you the address of the DNS server to use for DNS name and address resolution.

Discrete multitone (DMT) is a method for encoding digital data in an analog signal. By default, the ADSL interface uses Auto Detect mode, in which it automatically negotiates the DMT operating mode with the service provider DSLAM. You can change the mode on the adsl1 interface to force the interface to use only one of the following DMT standards:

- American National Standards Institute (ANSI) T1.413 Issue 2, which supports rates up to 8 Mbps downstream and 1 Mbps upstream.
- International Telecommunications Union (ITU) G.992.1 (also known as G.dmt), which supports minimum data rates of 6.144 Mbps downstream and 640 kbps upstream.
- ITU 992.2 (also known as G.lite), which supports up to data rates of 1.536 Mbps downstream and 512 kbps upstream. This standard is also called “splitterless DSL” because you do not have to install a signal splitter on your ADSL line (the service provider’s equipment splits the signal remotely).
Supported Port Modes

The port mode of a NetScreen-5GT ADSL device determines the binding of physical ports, logical interfaces, and zones.

- **Trust-Untrust port mode** (default)—This port mode uses the following default settings:
  - Binds the ADSL port to the adsl1 interface, which is bound to the Untrust zone.
  - Binds ethernet ports 1-4 to the ethernet1 interface, which is bound to the Trust zone.

- **Home-Work port mode**—Creates special Home and Work zones to segregate business and home users, while allowing users in both zones to access the Internet (the Untrust zone) through the ADSL interface. This port mode uses the following default settings:
  - Binds ethernet ports 1 and 2 to the ethernet1 interface, which is bound to the Work security zone.
  - Binds ethernet ports 3 and 4 to the ethernet2 interface, which is bound to the Home security zone.
  - Permits all traffic from the Work zone to the Untrust zone.
  - Permits all traffic from the Home zone to the Untrust zone.
  - Permits all traffic from the Work zone to the Home zone.
  - Denies all traffic from the Home zone to the Work zone (you cannot remove this policy)

In the Home-Work port mode, you must manage the device from the Work zone. You cannot configure the device from the Home zone, nor can you use any management services on the Home zone interface. The default IP address of ethernet1, the Work zone interface, is 192.168.1.1/24.

- **Trust-Untrust-DMZ port mode**—This port mode uses the following default settings:
  - Binds ethernet ports 1 and 2 to the ethernet1 interface, which is bound to the Trust security zone.
  - Binds ethernet ports 3 and 4 to the ethernet2 interface, which is bound to the DMZ security zone.
  - Binds the ADSL port to the adsl1 interface, which is bound to the Untrust security zone.

**NOTE:** The Trust/Untrust/DMZ port mode is supported only on the Extended version of the NetScreen-5GT ADSL device.
For all supported port modes, the adsl1 interface is the only interface bound to the Untrust zone by default.

You can change the port mode to use different port, interface, and zone bindings on the device. For more information about port modes, see the “Zones” chapter in the “Fundamentals” volume of the NetScreen Concepts & Examples ScreenOS Reference Guide.

Creating a Backup Link

When using ADSL, the adsl1 interface serves as the primary connection to the Internet. However, you can configure a backup connection to the Internet using the Untrusted ethernet port or the Modem port on the security device.

To configure the backup interface, bind both the adsl1 and backup interface to the Untrust zone to automatically configure the interface failover. If the ADSL interface becomes unavailable, the security device automatically sends outgoing traffic to the backup interface, which connects to the ISP account. When the ADSL interface is again available, the device automatically sends outgoing traffic to the adsl1 interface.

To configure the serial interface for the Modem, you must have the following information:

- Login and password for the account to the dialup service provider
- Primary phone connection for dialing into the account
- Modem initialization string

For more information about configuring the serial interface on a security device, see the “Interface Redundancy” chapter in the “High Availability” volume of the NetScreen Concepts & Examples ScreenOS Reference Guide.

For details on configuring the Modem and ISP settings for the serial interface in NetScreen-Security Manager, see “Configuring Modem Connection” on page 290.

For an example on configuring a backup link in an ADSL configuration, see “Configuring aDSL1 for PPPoE with Backup (Modem Port)” on page 273.

EXAMPLE: CONFIGURING ADSL1 TO ACCESS TO LOCAL SERVERS

In this example, you configure a NetScreen-5GT ADSL security device to permit internal hosts to access the Internet through the ADSL interface and permit Internet users to access a local Web server while protecting other internal hosts. To segregate traffic flow to the Web server from the rest of the internal network, configure the Web server in the DMZ, then create a firewall rule that permits HTTP traffic only to the DMZ zone.

NOTE: You can configure only one backup interface.

NOTE: All passwords handled by NetScreen-Security Manager are case-sensitive.
Figure 68: Access Internet Through ADSL Interface

1. Add the NetScreen-5GT ADSL security device as ADSL 1 (device name). To enable the DMZ zone, select the Trust/Untrust/DMZ port mode.

2. Configure the ADSL interface (ads1 interface in the Untrust zone):
   a. Double-click the device icon to open the device configuration. In the device navigation tree, select Network > Interface.
   b. Right click the ads1 interface and select Edit. The General Properties screen appears. Using the information you previously obtained from the service provider, configure the following:
      - For VPI, enter 0; for VCI, enter 35.
      - For Multiplexing Mode, select VC Multiplexing.
      - For IP address/netmask, enter 1.1.1.1/24
      - Ensure that Manageable is enabled.
      - Ensure that the Management IP is 1.1.1.1.
      - Ensure that the Mode is NAT
   c. In the interface navigation tree, select NAT > MIP. Configure the following:
      - For Mapped IP, enter 1.1.1.5.
- For Netmask, enter 32.
- For Host IP, enter 10.1.1.5.
- Ensure that the Host Virtual Router is set to trust-vr.

d. Click OK to add the MIP, then click OK again to save your changes to the ADSL interface.

3. Configure the Trust interface (ethernet1 in the Trust zone).
   a. Right-click ethernet1 and select Edit. The General Properties screen appears. Configure the interface to use an IP address and netmask of 192.168.1.1/24. For Interface Mode, select NAT.
   b. In the interface navigation tree, select DHCP. For DHCP Mode, select DHCP Server.
   c. Select the DHCP Server IP Pools tab, then configure the following:
      - For starting IP, enter 192.168.1.3.
      - For Value, select End IP.
      - For ending IP, enter 192.168.1.33.
   d. Click OK to add the new IP pool, then click OK again to save your changes to the Trust interface.

4. Configure the DMZ interface (ethernet2 in the DMZ zone).
   a. Double-click ethernet2. The General Properties screen appears. Configure the interface to use an IP address and netmask of 10.1.1.1/24. For Interface Mode, select NAT.
   b. Click OK to save your changes to the DMZ interface, then click OK to save and apply your changes to the device configuration.

5. Create a Global MIP to reference the MIP you created for the adsl1 interface. You use a Global MIP when configuring NAT in a Security Policy rule; the Global MIP references the MIP for an individual device, enabling you to use one object (the Global MIP object) to represent multiple MIPs in a single rule.

   a. In the navigation tree, select Object Manager > NAT Objects > MIP.
   b. Click the Add icon to display the new Global MIP dialog box.
   c. Configure the Global MIP as shown below:
6. Create a firewall rule that routes inbound HTTP traffic from any address in the Untrust zone to the MIP host (the Web server) in the DMZ zone. Configure the rule as shown below:

```plaintext
Figure 70: Create New Firewall Rule for HTTP Traffic
```

**EXAMPLE: CONFIGURING ADSL1 FOR PPPOA**

In this example, you configure a NetScreen-5GT ADSL security device to connect to the Internet using PPPOA and the ADSL interface. The device acts as both a PPPOA client and a DHCP server:

- As a PPPOA client, the device receives the IP address for the ADSL interface. However, the device also receives one or more IP addresses for DNS servers.
- As DHCP server, the device provides hosts in the Trust zone with their IP addresses and the IP addresses of the DNS servers.
1. **Add the NetScreen-5GT ADSL security device.**
   
   a. For device name, enter ADSL PPPoA
   
   b. Select Model Device.
   
   c. For device platform, select ns5GT adsl-Trust-Untrust

2. **Configure the ADSL Interface:**
   
   a. In the device navigation tree, select Network > Interface. Right-click the ADSL1 interface and select Edit. Configure the General Properties tab following:
      
      - For VPI, enter 0; for VCI, enter 35.
      
      - For Multiplexing Mode, select LLC/SNAP Encapsulation.
      
      - Ensure that Manageable is enabled and that the Management IP is 0.0.0.0.
      
      - Ensure that the zone is Untrust and the Mode is Route.
   
   b. Leave all other defaults and click OK to save your changes to the interface.

3. **Configure the Trust interface:**

---

**Figure 71: Example of PPPoA on ADSL Interface**

![Diagram of network setup with NetScreen-5GT ADSL security device, DSLAM, Internet access, DNS servers, DHCP range, and Trust/Untrust interfaces.](image)
a. Double-click the device icon to open the device configuration. In the device navigation tree, select Network > Interfaces.

b. Right-click ethernet1 and select Edit. The General Properties screen appears. Configure the interface to use an IP address and netmask of 192.168.1.1/24. For Interface Mode, select NAT.

c. In the interface navigation tree, select DHCP. For DHCP Mode, select DHCP Server.

d. Select the DHCP Server IP Pools tab, then configure the following:
   - For starting IP, enter 192.168.1.3.
   - For Value, select End IP.
   - For ending IP, enter 192.168.1.33.

e. Click OK to add the new IP pool, then click OK again to save your changes to the Trust interface.

4. Configuring the PPPoA instance:

   a. In the device navigation tree, select Network > PPPoA. Right-click the Trust interface and select Edit.

   b. Click the Add icon to create a new PPPoA instance, then configure the following:
      - For PPPoA Instance, enter poa1
      - For Interface, select the adsl1 interface.
      - For Username, enter Alex
      - For Password, enter tSOCbme4NW5iYPshGxCy67Ww48ngtHC0Bw==
      - Select Update DHCP Server.

   c. Leave all other defaults and click OK to save the PPPoA instance, then OK to save the device configuration.

After you have updated the device with the modeled configuration, the device administrator can activate PPPoA on local network.

- First, the device administrator powers down the NetScreen-5GTADSL security device and all workstations in the Trust zone, then powers on just the device. The device makes a PPPoA connection to the DSLAM, and obtains the IP address for the ADSL interface and the IP addresses for the DNS servers.

- Finally, the device administrator powers on the workstations to activate DHCP; the workstations automatically receive the IP address for the DNS server and obtain an IP address for themselves when they attempt a TCP/IP connection.
EXAMPLE: CONFIGURING ADSL1 FOR PPPOE WITH BACKUP (MODEM PORT)
In this example, you configure the NetScreen-5GTADSL security device as a firewall with the primary Internet connection through the ADSL interface using PPPoE, and a backup Internet connection through the serial modem port and dialup connection.

Figure 72: Example of PPPoE on ADSL Interface with Backup

1. Add the NetScreen-5GT ADSL security device.
   a. For device name, enter ADSL PPPoE.
   b. Select Model Device.
   c. For device platform, select ns5GT adsl-Home-Work.

2. Configure the ADSL Interface:
   a. In the device navigation tree, select Network > Interface. Right-click the ADSL1 interface and select Edit. Configure the General Properties tab:
      - For VPI, enter 0; for VCI, enter 35.
      - For Multiplexing Mode, select LLC/SNAP Encapsulation.
      - Ensure that the zone is Untrust and the Mode is Route.
   b. Leave all other defaults and click OK to save your changes to the ADSL interface.
3. Configure the Work interface:
   a. Double-click the device icon to open the device configuration. In the device navigation tree, select Network > Interfaces.
   b. Right-click ethernet1 and select Edit. The General Properties screen appears. Configure the interface to use an IP address and netmask of 192.168.1.1/24. For Interface Mode, select NAT.
   c. In the interface navigation tree, select DHCP. For DHCP Mode, select DHCP Server.
   d. Select the DHCP Server IP Pools tab, then configure the following:
      - For starting IP, enter 192.168.1.3.
      - For Value, select End IP.
      - For ending IP, enter 192.168.1.33.
   e. Click OK to add the new IP pool, then click OK again to save your changes to the Work interface.

4. Configure the Home interface:
   a. Double-click the device icon to open the device configuration. In the device navigation tree, select Network > Interfaces.
   b. Right-click ethernet2 and select Edit. The General Properties screen appears. Configure the interface to use an IP address and netmask of 192.168.2.1/24. For Interface Mode, select NAT.
   c. In the interface navigation tree, select DHCP. For DHCP Mode, select DHCP Server.
   d. Select the DHCP Server IP Pools tab, then configure a new DHCP IP Pool:
      - For starting IP, enter 192.168.2.2.
      - For Value, select End IP.
      - For ending IP, enter 192.168.2.5.
   e. Click OK to add the new IP pool, then click OK again to save your changes to the Home interface.

5. Configuring the PPPoE instance:
   a. In the device navigation tree, select Network > PPPoE. Right-click the Trust interface and select Edit.
   b. Click the Add icon to create a new PPPoE instance:
      - For PPPoE Instance, enter poe1
For Interface, select the ads1 interface.

For Username, enter Alex

For Password, enter tSOCbme4NW5iYPshGxCy67Ww48ntHC0Bw==

Select Update DHCP Server.

c. Leave all other defaults and click OK to save the PPPoE instance.

6. Configure the backup interface (the serial interface on the modem port):
   a. Double-click the device icon to open the device configuration. In the device navigation tree, select Network > Interfaces.
   b. Right-click serial interface and select Edit. The General Properties screen appears.
   c. For Zone, select Untrust.

7. Configure the ISP settings for the serial interface:
   a. In the device navigation tree, select Network > Dial > ISP.
   b. Create a new ISP and configure the following:
      ■ For ISP Name, enter isp1.
      ■ For Login Name, enter kgreen.
      ■ For Password, enter 98765432
      ■ For Primary Number, enter 4085551111
      ■ For Alternative Number, enter 4085552222
      ■ Ensure that the Priority is 1.
   c. Click OK to save the new ISP.

8. Configure the Modem settings for the serial interface:
   a. In the device navigation tree, select Network > Dial > Modem.
   b. Select the Modem tab and configure the following:
      ■ For Modem Name, enter mod1.
      ■ For Init String, enter AT&FS7=255S32=6
      ■ Select Is Active.
c. Click OK to save the new modem settings, then click OK again to save your changes to the device configuration.

**NOTE:** The ISP and Modem settings automatically apply to the serial interface; you do not need to manually assign them to the Modem port.

---

### Configuring a Wireless Interface

A wireless interface handles wireless traffic on a NetScreen-5GT Wireless security device that is configured as a wireless access point (WAP). The wireless interfaces are prebound to security zones as detailed below.

**Table 15: Wireless Interface-to-Zone Mapping**

<table>
<thead>
<tr>
<th>Wireless Interfaces</th>
<th>Security Zones</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless1</td>
<td>Wzone1</td>
</tr>
<tr>
<td>Wireless2</td>
<td>Trust or Work (binding depends on port mode)</td>
</tr>
<tr>
<td>Wireless3</td>
<td>DMZ or Home (binding depends on port mode)</td>
</tr>
<tr>
<td>Wireless4</td>
<td>Wzone2 (available only on the NetScreen-5GT Wireless security device with Extended license key and Extended port mode)</td>
</tr>
</tbody>
</table>

Each wireless interface must use a separate subnet from all other wireless and wired interfaces. To shutdown an interface, enable the option Shutdown Interface in the General Properties for the interface.

To enable the wireless interface to handle wireless traffic, you must associate the interface with a service set identifier (SSID). The SSID links its basic service set (BSS) with the interface, which in turn is prebound to a security zone. Because there can be only one BSS per security zone, the rules you apply to that zone also apply to the BSS in that zone. For details on binding a wireless interface to an SSID, see “Configuring Wireless SSIDs” on page 160.

---

### Configuring DIP Groups

Use a DIP group to combine two DIP pools for two security devices that are in an active/active NRSP configuration. When specifying the NAT settings in the rule options for a Security Policy rule, you can select a DIP group instead of a single DIP pool.

Selecting a DIP group in the policy enables NAT using the DIP pool that exists on either device in the HA configuration. Typically, two security devices in an active/active configuration share the same configuration, and both devices process traffic simultaneously. When you define a policy to perform NAT using a DIP pool located on one VSI, because that VSI is active only on the device acting as the master of the VSD group to which the VSI is bound, any traffic sent to the other device—the one acting as the backup of that VSD group—cannot use that DIP pool and is dropped. To solve this problem, you can create two DIP pools—one on the Untrust zone VSI for each VSD group—and combine the two DIP pools into one DIP group, which you reference in the policy. Each VSI uses its own VSD pool even though the policy specifies the DIP group.
If you do not use a DIP group, the security device that acts as the backup of a VSD group cannot use a DIP pool located on the VSI of the master of the VSD group. For more details about DIP groups on security devices, see the “Fundamentals” volume in the NetScreen Concepts & Examples ScreenOS Reference Guide.

EXAMPLE: CONFIGURING A DIP GROUP ON THE DEVICE

In this example, you configure a DIP group that includes the DIP pools of two security devices in an active/active NSRP configuration. By combining the DIP pools located on both Untrust zone VSIs (for VSD groups 0 and 1) into one DIP group, Devices A and B can both process traffic matching policy “out-nat”, which references not an interface-specific DIP pool but the shared DIP group.

Figure 73: Example of DIP Group Configuration

1. Create the Cluster:
   a. In the navigation tree, select Device Manager > Security Devices. Click the Add icon and select Cluster. Configure the Cluster as shown below:
2. Configure the untrust interface for VSD group 0.
   a. In the cluster navigation tree, select Network > Interface.
   c. Configure the IP address as 1.1.1.1 and the Netmask as 24. Leave all other settings as default.
   d. Select NAT > DIP to display the Dynamic IP dialog box. Configure the following and click OK:
      - For DIP ID, enter 5.
      - For Start, enter 1.1.1.20.
      - For End, enter 1.1.1.29.
   e. Click OK to save your changes.

3. Configure the trust interface for VSD group 0.
   a. In the cluster navigation tree, select Network > Interface.
   c. Configure the IP address as 10.1.1.1, the Netmask as 24. Leave all other settings as default.
   d. Click OK to save your changes.

4. Configure the untrust interface for VSD group 1:
a. In the cluster navigation tree, select Network > Interface.

b. Right-click ethernet3 and select New > VSI.

c. Configure the IP address as 1.1.1.2, the Netmask as 24. Leave all other settings as default, as shown below:

Figure 75: Configure IP Address

<table>
<thead>
<tr>
<th>General Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>IP Options</td>
</tr>
<tr>
<td>IP Address</td>
</tr>
<tr>
<td>Netmask</td>
</tr>
<tr>
<td>Manageable</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interface Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
</tr>
</tbody>
</table>

d. Select NAT > DIP to display the Dynamic IP dialog box. Configure the following and click OK:

- For DIP ID, enter 6.
- For Start, enter 1.1.1.30.
- For End, enter 1.1.1.39.

e. Click OK to save your changes.

5. Configure the trust interface for VSD group 1.

a. In the cluster navigation tree, select Network > Interface.

b. Right-click ethernet1 and select New > VSI.

c. Configure the IP address as 10.1.1.2, the Netmask as 24. Leave all other settings as default.

d. Click OK to save your changes.

6. Create the DIP group:

a. In the cluster navigation tree, select Network > DIP Group.

b. Click the Add icon in the DIP Group configuration screen. The Dynamic IP dialog box appears.

c. Configure the DIP Group Name as 7, and select DIP members 5 and 6.
d. Click OK to close the Dynamic IP dialog box, then click OK to close save your changes.

7. Select DIP Translation Stickiness to ensure that the device assigns the same IP address from a DIP pool to a host for multiple concurrent sessions.
   a. In the cluster navigation tree, select Network > Advanced > DIP.
   b. Select DIP Translation Stickiness.
   c. Click OK to save your changes.

For details on DIP Translation Stickiness, see “Configuring DIP Options” on page 298.

8. Create a Global DIP to reference the DIP group for the cluster. You use a Global DIP when configuring NAT in a firewall rule; the Global DIP references the DIP pool or DIP group for an individual device or cluster, enabling you to use one object (the Global DIP object) to represent multiple DIP pools or DIP groups in a single rule.
   a. In the navigation tree, select Object Manager > NAT Objects > DIP.
   b. Click the Add icon to display the new Global DIP dialog box.
   c. Configure the Global DIP as shown below:

   ![Configure New Global DIP](image)

   d. Click OK to save your changes.
9. Configure a firewall rule to use the Global DIP object for NAT translation, as shown below:

Figure 77: Configure Firewall Rule to Use Global DIP Object

<table>
<thead>
<tr>
<th>Match</th>
<th>Action</th>
<th>Install Or</th>
<th>Rule Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>From Zone</td>
<td>Source</td>
<td>To Zone</td>
<td>Destination</td>
</tr>
<tr>
<td>trust</td>
<td>any</td>
<td>untrust</td>
<td>any</td>
</tr>
</tbody>
</table>

Configuring PPP

Use the PPP option to configure how the device handles Point-to-Point Protocol (PPP) connections. PPP encapsulation allows different Network Layer protocols to be multiplexed simultaneously over commonly used physical links. To establish a PPP connection, you configure each end of a PPP link by exchanging Link Control Protocol (LCP) packets. LCP is used to establish, configure, and test data-link options. These options include encapsulation format options, authentication of the peer on the link, handling of varying limits on sizes of packets, detecting a looped-back link and other common misconfiguration errors; determining when a link is functioning properly or failing; and terminating the link.

PPP allows for authentication during link establishment to permit or deny connection to a device. This authentication can be performed using either Password Authentication Protocol (PAP) or Challenge-Handshake Authentication Protocol (CHAP). These authentication protocols are intended for use primarily by hosts and routers that connect to a network server via switched circuits or dial-up lines but can also be used with dedicated lines.

For an interface with PPP encapsulation, you must configure a PPP access profile and bind it to the interface. You create an access profile with a user-defined name that is unique on the SSG device. You can bind the same access profile to more than one interface, but only one profile can be assigned to an interface. A PPP access profile includes the following information:

- PPP Profile Name
- Auth Local Name
Configuring PPPoE

Use the PPPoE option to configure how the device handles Point-to-Point Protocol over Ethernet (PPPoE) connections. PPPoE enables multiple users at a site to share the same digital subscriber line, cable modem, or wireless connection to the Internet. Some security devices support PPPoE, which enables them to operate compatibly on DSL, Ethernet Direct, and cable networks run by ISPs that use PPPoE for their clients’ Internet access.

**NOTE:** Some ISPs use DHCP for their clients’ Internet access. To configure DHCP on an interface, see “Configuring DHCP” on page 229. For more detailed explanation about PPPoE or DHCP on security devices, see the “Fundamentals” volume in the NetScreen Concepts & Examples ScreenOS Reference Guide.

On devices that support PPPoE, you can configure a PPPoE client instance on any or all interfaces. You configure a specific instance of PPPoE with a user name and password and other parameters, and bind the instance to an interface. When two Ethernet interfaces (a primary and a backup) are bound to the Untrust zone, you can configure one or both interfaces for PPPoE. Specifically:

- For low-end security devices running ScreenOS 4.0.3 or earlier, you can only enable PPPoE on a single interface bound to the Untrust zone. This restriction applies to the following devices: NetScreen-5XT, NetScreen-5XP, NetScreen-25, NetScreen-50, NetScreen-100, NetScreen-204, and NetScreen-208.

- For all security devices running ScreenOS 5.0, you can enable PPPoE on multiple interfaces in any zone at the same time.

- For all security devices running ScreenOS 5.1 and higher, you can bind a PPPoE instance to a:
  - VSI interface. Use this option when running two devices using NSRP in Active-Passive mode: When failover occurs, the new master device can use the same IP as the previous master device to continue communicating with the ISP. Because the PPPoE connection is maintained, downtime during failover is minimized. To bind PPPoE instance to a VSI interface, you must have already created the NSRP cluster and the VSI interfaces.
Subinterface. Use this option to enable multiple PPPoE sessions on one physical interface. To bind the PPPoE instance to a subinterface, you must have already created the subinterface. For details, see “Configuring a Subinterface” on page 260. For an example on configuring multiple PPPoE sessions on a single interface, see “Configuring Multiple PPPoE Instances on a Single Interface” on page 286.

### Automatic Update of DNS Servers

When you initiate a PPPoE connection, your ISP automatically provides the IP addresses for the Untrust zone interface and the IP addresses for the Domain Name Service (DNS) servers. When the device receives DNS addresses via PPPoE, the new DNS settings overwrite the local settings by default.

If you do not want the new DNS settings to replace the local settings, enable the setting Manual IP Configuration when configuring a PPPoE instance. If you use a static IP address for the Untrust zone interface, you must obtain the IP addresses of the DNS servers and manually enter them on the security device and on the hosts in the Trust zone.

**EXAMPLE: CONFIGURING PPPOE AND DHCP**

In this example, the security device receives a dynamically assigned IP address for its Untrust zone interface (ethernet3) from the ISP. Because the device also dynamically assigns IP addresses for the three hosts in its Trust zone, the device acts both as a PPPoE client and a DHCP server. The Trust zone interface must be in either NAT mode or Route mode. In this example, it is in NAT mode.

Before setting up the site in this example for PPPoE service, you must have the following: a Digital subscriber line (DSL) modem and line, an account with an ISP, and a user name and password (obtained from the ISP).

1. Add a NetScreen-5GT device running 5.0 named “Device A”.
2. Configure the ethernet1 interface (Trust Interface):
a. In the device navigation tree, select Network > Interface.

b. Double-click the ethernet1 interface. The General Properties screen appears.

c. Configure the General Properties:
   - For Zone, select Trust (default setting).
   - For IP Address, enter IP Address 172.16.30.10.
   - For Netmask, enter 24
   - Ensure that Manageable is enabled and that the Management IP is 172.16.30.10.
   - For Interface Mode, select NAT (default setting).

d. In the interface navigation tree, select DHCP. Set the DHCP mode to DHCP Server and configure as shown below:

Figure 79: Configure Ethernet1 DHCP Server Settings

<table>
<thead>
<tr>
<th>Server Settings</th>
<th>Custom Options</th>
<th>IP Pools</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP Server Auto Probing</td>
<td>□ disable DHCP server</td>
<td></td>
</tr>
<tr>
<td>DNS #1</td>
<td>0.0.0.0</td>
<td></td>
</tr>
<tr>
<td>DNS #2</td>
<td>0.0.0.0</td>
<td></td>
</tr>
<tr>
<td>DNS #3</td>
<td>. . .</td>
<td></td>
</tr>
<tr>
<td>Domain Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client Gateway</td>
<td>0.0.0.0</td>
<td></td>
</tr>
<tr>
<td>Lease Time (Minutes)</td>
<td>60 △</td>
<td></td>
</tr>
<tr>
<td>Netmask</td>
<td>none △</td>
<td></td>
</tr>
</tbody>
</table>

   - For DNS #1, DNS #2, and Client Gateway, enter 0.0.0.0
   - For Lease Time, enter 60 (60 minutes).
   - Leave all other defaults

e. Select the IP Pools tab, then click the Add icon. the New DHCP IP Pool dialog box appears. Configure the following:
   - For IP Address, enter 172.16.30.2
   - For Value, select End IP.
   - For End of Dynamic IP Range, enter 172.16.30.5

f. Click OK to save the new IP Pool, then click OK to save your changes to the interface.
3. Configure the ethernet3 interface (Untrust Interface):
   a. In the device navigation tree, select Network > PPPoE.
   b. Click the Add icon. The New PPPoE Instance dialog box appears. Configure the following:
      - For PPPoE Instance, enter eth3-pppoe.
      - For Interface, select ethernet3.
      - For username, enter user1.
      - For password, enter 123456.
      - For Concentrator-Name, enter ac-11
      - Leave all other defaults.
   c. Click OK to add the instance, then click OK again to save your changes to the device.

4. Activate PPPoE and DHCP on the network:
   a. Turn off the power to the DSL modem, the security device, and any connected workstations.
   b. Turn on the DSL modem.
   c. Turn on the security device. The device makes a PPPoE connection to the ISP and, through the ISP, gets the IP addresses for the DNS servers.
   d. To activate DHCP on the Internal Network, turn on the workstations. The workstations automatically receive the IP addresses for the DNS servers. They get an IP address for themselves when they attempt a TCP/IP connection. Every TCP/IP connection that a host in the Trust zone makes to the Untrust zone automatically goes through the PPPoE encapsulation process.

Configuring Multiple PPPoE Sessions on a Single Interface

Some security devices support multiple PPPoE sub-interfaces (each with the same MAC address) for a given physical interface. On such devices, you can make a PPPoE connection on multiple instances by binding each sub-interface to a different PPPoE instance. You can determine which traffic the device sends over a particular PPPoE session by configuring routes that specify a specific PPPoE sub-interface for each session (no rules determine the flow of traffic). IPSec tunnels can terminate on such PPPoE sub-interfaces.

The maximum number of concurrent PPPoE sessions on a physical interface is limited only by number of sub-interfaces allowed by the device. There is no restriction on how many physical interfaces can support multiple sessions. You can specify username, static-ip, idle-timeout, auto-connect and other parameters separately for each PPPoE instance or session.
To support a PPPoE session, a sub-interface must be untagged. A tagged sub-interface uses an associated VLAN tag to enable the sub-interface to receive Layer 2 traffic and direct it selectively to a particular VLAN, which usually resides in a trusted zone. VLAN tags allow a single physical interface to direct exchanged packets selectively to and from VLANs, each through a different sub-interface.

By contrast, an untagged interface does not use a VLAN tag to identify a VLAN for a sub-interface. Instead, it uses a feature called encap, which binds the sub-interface to a particular defined PPPoE definition. By hosting multiple sub-interfaces, a single physical interface can host multiple PPPoE instances. You can configure each instance to go to a specified AC (Access Concentrator), thus enabling separate entities (such as ISPs) to manage the PPPoE sessions through a single interface.

**EXAMPLE: CONFIGURING MULTIPLE PPPOE INSTANCES ON A SINGLE INTERFACE**

In the following example you define three PPPoE instances:

- **Instance isp_new_york**, password “swordfish”, bound to interface ethernet3. This instance provides access to a service named “Big_Apple_Service”. The AC is named “isp_ny_ac”.

- **Instance isp_los_angeles**, password “marlin”, bound to sub-interface ethernet3.1. This instance provides access to a service named “Angels_Service”. The AC is named “isp_la_ac”.

- **Instance isp_chicago**, password “trout”, bound to sub-interface ethernet3.2. This instance provides access to a service named “Windy_City_Service”. The AC is named “isp_c_ac”.

Figure 80: Configuring Multiple PPPoE Instances on an Interface
3. In the device navigation tree, select Network > Interfaces. Configure the subinterfaces for the Los Angeles and Chicago ISPs:

   a. Click the Add icon and select Sub Interface. The General Properties screen appears. Configure as shown below:

   Figure 81: Configure Sub Interface for Los Angeles on Ethernet3

<table>
<thead>
<tr>
<th>General Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name: ethernet3, Tag: 1, Sub Interface Type: encap, Encap: pppoe</td>
</tr>
</tbody>
</table>

   - For Name, select ethernet 3.
   - For Tag, select 1.
   - For Sub Interface Type, select encap.
   - For Encap, select pppoe.
   - For Zone, select Untrust.

   Leave all other defaults and click OK to save the new Sub Interface.

   b. Click the Add icon and select Sub Interface. The General Properties screen appears. Configure as follow:

   - For Name, select ethernet 3.
   - For Tag, select 2.
   - For Sub Interface Type, select encap.
   - For Encap, select pppoe.
   - For Zone, select Untrust.

   Leave all other defaults and click OK to save the new Sub Interface.

4. Configure the PPPoE Instance for the New York ISP:

   a. In the device navigation tree, select Network > PPPoE.

   b. Click the Add icon. The New PPPoE Instance dialog box appears. Configure the following, then click OK:

   - For Name, enter isp_new_york.
   - For Interface, select the physical interface ethernet3.
   - For Username, enter user1@domain1.
- For Password, enter swordfish.
- For Access Concentrator, enter isp.ny_ac
- For Service, enter Big_Apple_Service.
- Select Clear On Disconnect.
- Leave all other defaults.

5. Configure the PPPoE Instance for the Los Angeles ISP:
   a. In the device navigation tree, select Network > PPPoE.
   b. Click the Add icon. The New PPPoE Instance dialog box appears. Configure the following then click OK:
      - For Name, enter isp.los_angeles.
      - For Interface, select the subinterface ethernet3.1.
      - For Username, enter user2@domain2.
      - For Password, enter marlin.
      - For Access Concentrator, enter isp_la_ac
      - For Service, enter Angels_Service.
      - Select Clear On Disconnect.
      - Leave all other defaults.

6. Configure the PPPoE Instance for the Chicago ISP:
   a. In the device navigation tree, select Network > PPPoE.
   b. Click the Add icon. The New PPPoE Instance dialog box appears. Configure the following, then click OK:
      - For Name, enter isp.chicago.
      - For Interface, select the subinterface ethernet3.2.
      - For Username, enter user3@domain3.
      - For Password, enter trout.
      - For Access Concentrator, enter isp_c_ac
      - For Service, enter Windy_City_Service.
      - Select Clear On Disconnect.
      - Leave all other defaults.
c. Click OK to save your changes to the device.

Configuring PPPoA

PPPoA is typically used for PPP sessions that terminate on a security device with an ADSL interface (the NetScreen-5GT ADSL security device). On the ADSL interface (or its subinterfaces), you can configure a PPPoA client instance with a user name, password, and other parameters, then bind the instance to the ADSL interface (or subinterface).

When the NetScreen-5GT ADSL security device initiates a PPPoA connection to the PPPoA server (controlled by the service provider), the server automatically provides the IP addresses for the Untrust zone interface and for the Domain Name Service (DNS) servers. Using this information, the security device automatically updates the DNS server addresses in its DHCP server (you can disable this automatic update if desired).

For details and an example of configuring an ADSL interface with PPPoA, see “Configuring an ADSL Interface” on page 264.

Configuring NACN

Use the NACN option to configure NetScreen Address Change Notification (NACN). NACN is available only on security devices running ScreenOS 4.0.x. Before NetScreen-Security Manager can contact a security device, it must have the current IP address of the device interface. This is relatively easy when the security device has a static IP address on its interface. However, an interface on a security device can have a dynamically assigned IP address, using either PPPoE or DHCP. In these cases, the security device uses NACN to monitor a specific interface and then register with NetScreen-Security Manager the IP address of the interface whenever it changes. This prevents interruption of communication between NetScreen-Security Manager and the security device.

For more detailed explanation about NACN on security devices, see the “Administration” volume in the JNetScreen Concepts & Examples ScreenOS Reference Guide for ScreenOS 4.0.0.

Configuring Interface Failover

(This option is only available for some security devices.) Use the Failover option to configure the security device to switch over traffic from the primary interface to the backup interface, and from the backup to the primary when there are both primary and backup interfaces bound to the Untrust zone. An interface failover can occur when ScreenOS detects a physical link problem on the primary interface connection, such as an unplugged cable. You can also define the following types of interface failover:

- When certain IP addresses become unreachable through a given interface using IP tracking
- When certain VPN tunnels on the primary untrust interface become unreachable using VPN tunnel monitoring
You can also configure the security device to automatically switch to the backup interface if ScreenOS detects a failure on the primary interface connection. When the connection through the primary interface is restored, ScreenOS automatically switches traffic from the backup interface to the primary.

By default, there is a 30-second interval before the failover occurs (the hold-down time). You can change this interval.

For more detailed explanation about interface failover on security devices, see the “High Availability” volume in the NetScreen Concepts & Examples ScreenOS Reference Guide or the New Features Guide for ScreenOS 4.0.0-DIAL2.

Configuring Modem Connection

(This option is only available for some security devices.) Use the Modem option to configure the security device for operation with an external modem. You can connect an external modem to the RS-232 serial port on certain security devices to enable the device to establish a PPP connection to an ISP. This provides a backup serial interface for traffic to the Untrust zone if there is a failure on the connection through the primary interface.

You can configure the following parameters for the serial link:

- **Speed (BPS)**—The maximum baud rate for the serial link (the default rate is 115200 bps).
- **Timeout**—The maximum amount of time that the serial link can be idle before ScreenOS automatically disconnects the modem (the default is 10 minutes).
- **Retry Number**—The number of times ScreenOS retries the dial-up connection if the line is busy or there is no response (the default is 3 times).
- **Retry Interval**—The interval, in seconds, between dial-up retries (the default is 10 seconds).

Creating Modem Settings

The modem you use for the dial-up connection must support the following features:

- **Hardware flow control**
- **Provide clear to send (CTS) signals**
- **Able to respond to request to send (RTS) signals**
- **Asynchronous only**
- **Support AT command set**

To create the settings for a modem:

1. Click the Add icon in the Modem Settings portion of the Modem configuration screen.
2. Specify the name for the modem setting.

3. Specify the modem initialization string. The modem initialization string must meet the following requirements:
   - Hardware flow control is recommended, but not required (you can specify no flow control)
   - Software flow control is not used
   - Result code must be displayed in verbal mode

4. Specify whether this modem setting is active. You can activate only one of the configured modem settings at a time.

5. Click OK.

Creating ISP Settings

You configure the security device to dial to an ISP account if a failover to the serial interface occurs and there is traffic to be sent. You can configure up to four ISP connections, assigning each a different priority number (1 is the highest priority). The priority number determines the order that the device uses in attempting the dial-up connection; the ISP with the highest priority is dialed first. If the device is unable to log in to the ISP account with the highest priority, it dials the ISP with the next highest priority number, and so on, until there are no more ISP configurations.

To create the settings for a ISP connection:

1. Click the Add icon in the ISP Settings portion of the Modem configuration screen.

2. Specify the name for the ISP setting.

3. Specify the login name and password for the ISP account.

4. Specify the primary phone number and optionally, an alternate phone number.
   If the modem uses pulse dial by default but you want to use tone dial, precede the phone number with a T. If the modem uses tone dial by default but you want to use pulse dial, precede the phone number with a P.

5. Specify the priority for this setting, relative to other configured ISP settings. The highest priority is 1.

6. Click OK.

For more detailed explanation about interface failover on security devices, see the “High Availability” volume in the NetScreen Concepts & Examples ScreenOS Reference Guide or the New Features Guide for ScreenOS 4.0.0-DIAL2.
Setting ISP Priority for Failover

When using a modem connection, a trustee administrator can manually change an ISP priority. If a failover situation occurs, the priority assigned to an ISP indicates in what order relative to other ISPs that a particular ISP will be contacted. The lower the value, the higher the priority of the ISP. The trustee admin can also check the availability of an ISP with a priority setting of zero (0).

A root administrator (not a trustee admin), can configure up to four ISPs. The priority of each ISP must be a unique number. You can also configure more than one ISP with a priority of zero.

Configuring DNS

Use the DNS option to configure DNS server information. Before the security device can use DNS for domain name/address resolution, you must configure the address for the primary DNS server the device should use.

Configuring DNS Settings

Specify the IP addresses for a Primary DNS server and a Secondary DNS server, then specify a refresh interval. You can configure the device to refresh all the entries in its DNS table by checking them with a specified DNS server at a specified time of day at regularly scheduled intervals. Alternatively, you can select Never Refresh to ensure that the device does not update its DNS table.

NOTE: The device automatically attempts to refresh its DNS table after an HA failover occurs.

For more detailed explanation about configuring DNS on security devices, see the “Fundamentals” volume in the NetScreen Concepts & Examples ScreenOS Reference Guide.

Configuring DNS Proxy

Use a DNS proxy to enable split DNS queries. The proxy selectively redirects the DNS queries to specific DNS servers according to partial or complete domain names. This is useful when VPN tunnels or PPPoE virtual links provide multiple network connectivity, and it is necessary to direct some DNS queries to one network, and other queries to another network.

NOTE: You can configure DNS Proxy for the root device in a Vsys, but not for the individual Vsys devices.

You can use DNS proxies to make domain lookups more efficient. For example, to reduce load on the corporate server, you can route DNS queries meant for the corporate domain to the corporate DNS server, while routing other DNS queries to the ISP DNS server. You can also use DNS proxy to transmit selected DNS queries through a tunnel interface, preventing malicious users from learning about internal network configuration.
To use a DNS proxy, you must:

- Select DNS proxy on the device, in the DNS Proxy Setting screen, and
- Select DNS proxy on the interface, in the interface General Properties screen.

Additionally, you should also point the DNS servers (defined in DNS Settings) to the loopback IP address (127.0.0.1).

**To configure a DNS proxy to use a default DNS server, set the Domain Name as the asterisk character (*) for the default DNS Proxy, then select the “failover” option for all non-default DNS Proxies.**

**EXAMPLE: CONFIGURING DNS PROXIES**

In this example, you create two DNS proxy entries that selectively forward DNS queries to different servers:

- A DNS query with a FQDN containing the domain name acme.com goes out tunnel interface tunnel.1 to the corporate DNS server at 2.1.1.21. When a host sends a DNS query to the www.acme.com, the device automatically directs the query to this server, which resolves the query to 3.1.1.2.

- A DNS query with a FQDN containing the domain name acme_eng.com goes out tunnel interface tunnel.1 to the DNS server at 2.1.1.34. When a host sends a DNS query to the intranet.acme_eng.com, the device directs the query to this server, which resolves the query to 3.1.1.5.

- All other DNS queries bypass the corporate servers and go out interface ethernet3 to the DNS server at 1.1.1.23. When the host and domain name is www.juniper.net, the device automatically bypasses the corporate servers and directs the query to this server, which resolves the query to 207.17.137.68.

**Figure 82: Configuring DNS Proxies Example Overview**

1. Add a NS-208 security device running ScreenOS 5.1.

2. In the main navigation tree, select Device Manager > Security Devices, then double-click the device to open the device configuration.
3. **Add the tunnel.1 interface:**
   a. In the device navigation tree, select Network > Interface.
   b. Click the Add icon and select tunnel interface.
   c. Click OK to save the new interface.

4. **Configure the Trust interface:**
   a. In the device navigation tree, select Network > Interface.
   b. Double-click the trust interface. The General Properties screen appears.
   c. Select Enable DNS Proxy.
   d. Click OK to save the new interface.

5. **Configure general DNS Proxy settings:**
   a. In the device navigation tree, select Network > DNS > DNS Proxy.
   b. Select Configure DNS Proxy Instance.
   c. Select Enable.

6. **Add the DNS Proxy for acme.com:**
   a. Click the Add icon. The New DNS Proxy dialog box appears.
   b. Configure as shown below, then click OK:
      - For Domain Name, enter .acme.com
      - For Outgoing Interface, enter tunnel.1
      - For Primary DNS Server, enter 2.1.1.21
      - Select Failover.

7. **Add the DNS Proxy for acme_eng.com:**
   a. Click the Add icon. The New DNS Proxy dialog box appears.
   b. Configure as shown below, then click OK:
      - For Domain Name, enter .acme_eng.com
      - For Outgoing Interface, enter tunnel.1
      - For Primary DNS Server, enter 2.1.1.34
      - Select Failover.

8. **Add the DNS Proxy for all other DNS requests:**
a. Click the Add icon. The New DNS Proxy dialog box appears.

b. Configure as shown below:
   - For Domain Name, enter *
   - For Outgoing Interface, enter ethernet3
   - For Primary DNS Server, enter 1.1.1.23

9. Click OK to save your changes to the device.

Configuring Dynamic DNS

Use Dynamic DNS (DDNS) to enable client devices to dynamically update IP addresses for registered domain names. You might want to use DDNS for a security device that dynamically receives its IP address from an ISP via PPP, DHCP, or XAuth. When the device is protecting a web server, clients from the internet can access that web server using a domain name, even if the IP address of the security device changes.

A DDNS server stores dynamically-changed addresses and associated domain names. To use DDNS, you must set up an account, including username and password, with the DDNS server, such as dyndns.org or ddo.jp. The security device updates DDNS servers with the account information periodically, or in response to IP address changes, and the DDNS server uses the account information to configure client devices.

To control how often the device updates the DDNS server, set the number of minutes between DDNS updates. The default (and recommended) value is 60 minutes; accepted range is 1-1440. However, the device might not update at every interval because the DNS server must first timeout the DDNS entry from its cache. If you set the Minimum Update Interval too low, the security device may lock you out.

EXAMPLE: CONFIGURING DYNAMIC DNS (DDNS)

In this example, you configure a security device to use the DDNS server dyndns.org for resolving changed addresses. In the DDNS settings, you define the web server as the protected host, then bind the host to the source interface (ethernet3). When the device sends an update to the ddo.jp server, the host name (www.my.host.com) is associated with the interface (ethernet3).

NOTE: You can configure Dynamic DDNS for the root device in a Vsys, but not for the individual Vsys devices.
Figure 83: Configuring DDNS Example Overview

1. Add an NS-208 security device running ScreenOS 5.1.

2. In the main navigation tree, select Device Manager > Security Devices, then double-click the device to open the device configuration.

3. Configure general Dynamic DNS settings:
   a. In the device navigation tree, select Network > DNS > Dynamic DNS.
   b. Select Configure Dynamic DNS Instance.
   c. Select Enable Dynamic DNS.

4. Add the DDNS instance for the web server:
   a. Click the Add icon. The New Dynamic DNS dialog box appears.
   b. Configure as shown below:

Note: The Untrust zone is not shown.
Configuring Advanced Network Settings

In the Advanced Network screens, you can configure the following network settings:

- Configuring ARP Cache Entries

For ID, enter 12.

- For Server Type, select dyndns.

- For FQDN Server Name, enter dyndns.org.

- For Refresh Interval (Hours), enter 24.

- For Minimum Update Interval (Minutes), enter 15.

- For User Name of DDNS Account, enter swordfish.

- For Password for DDNS Account, enter ad93lvb.

- For Source Interface, select ethernet3.

- For Host Name, enter www.my_host.com.

c. Click OK to save the new DDNS instance, then click OK to save your changes to the device.

NOTE: You do not need to enter an Agent Name. The security device automatically generates the agent name using internal information, such as the ScreenOS version, serial name, and platform.

Configuring Advanced Network Settings
Configuring ARP Cache Entries

Use the ARP option to manually add entries to the Address Resolution Protocol (ARP) cache. The ARP cache contains associations of IP addresses to physical machine addresses known as Media Access Control (MAC) addresses. The ARP normally resolves unknown IP addresses and updates its cache automatically. You can manually add ARP cache entries, if necessary, for testing or troubleshooting purposes.

To add an ARP cache entry:

1. Click the Add icon in the ARP configuration screen.
2. Specify the IP address, interface, and MAC address for the ARP entry.
3. Click OK.

For more detailed explanation about configuring ARP entries on security devices, see the `arp` commands in the NetScreen CLI Reference Guide.

Configuring VIP Options

A virtual IP (VIP) address maps traffic received at one IP address to another address based on the destination port number in the TCP or UDP segment header. You can only set a VIP on an interface in the Untrust zone. The IP address for the VIP must be in the same subnet as an interface in the Untrust zone. (On some security devices, the IP address for the VIP can be the same address as the Untrust zone interface.) In addition, you need the following information to define a VIP:

- The IP addresses for the servers that process the requests
- The type of service you want the security device to forward from the VIP to the IP address of the host.

Use the VIP Options configuration screen to set multiple port entries for VIPs. A single VIP can support custom services with multiple port entries by creating multiple service entries under that VIP. To be able to use multiple-port services in a VIP, you need to enable multiple port services, then reset the security device.

For more detailed explanation about configuring VIPs on security devices, see the “Fundamentals” volume in the NetScreen Concepts & Examples ScreenOS Reference Guide.

Configuring DIP Options

Use DIP Options to set DIP translation operation.
When DIP is configured on an interface, the security device normally assigns a different source IP address for each session, even when a single host initiates several sessions that require network address translation using the DIP pool. This random address assignment can be problematic for services that create multiple sessions that require the same source IP address for each session.

For example, it is important to have the same IP address for multiple sessions when using the AOL Instant Messaging (AIM) client. You create one session when you log in, and another for each chat. For the AIM server to verify that a new chat belongs to an authenticated user, it must match the source IP address of the login session with that of the chat session. If they are different—possibly because they were randomly assigned from a DIP pool during the NAT process—the AIM server rejects the chat session.

To ensure that the device assigns the same IP address from a DIP pool to a host for multiple concurrent sessions, enable DIP Translation Stickiness.

For more detailed explanation about configuring DIP options on security devices, see the “Fundamentals” volume in the NetScreen Concepts & Examples ScreenOS Reference Guide.

For details about creating a DIP group, see “Configuring DIP Groups” on page 276.

Configuring Device Administration

Use the Device Administration screens to configure administrative options for the managed device. In the device navigation tree, select Device Admin to view configuration options.

This section describes configuring the following device administration options for security devices:

- Configuring Device Administrators
- Configuring Permitted IPs
- Configuring CLI Management
- Configuring Web Management
- Configuring Date and Time Settings

For more detailed explanation about configuring device administration on security devices, see the “Fundamentals” and “Administration” volumes in the Juniper NetScreen Concepts & Examples ScreenOS Reference Guide.
Configuring Device Administrators

A device administrator is the person responsible for managing a device locally using ScreenOS (command line or WebUI). A security device includes one default device administrator account, the root device administrator, which has complete access to all functionality on the device. Using NetScreen-Security Manager, you can create 20 additional device administrators with different privilege levels.

NOTE: To enable a device administrator to use NetScreen-Security Manager to manage devices, you must create a NetScreen-Security Manager administrator account for the device admin. For details, see “Creating Administrators” on page 57.

When you import a device configuration into NetScreen-Security Manager, device administrator accounts are not automatically imported—you must manually import the accounts from the device using a separate directive. You cannot manage device administrator functionality in NetScreen-Security Manager until you have imported the device administrator information from the physical device (the device admin screens do not appear).

To notify you when device admin information needs to be imported, NetScreen-Security Manager displays the message “Need to Migrate Admin Info From Device”. To view this message, in the device navigation tree, select Device Administration; the message appears in the main display area. When present, this message indicates that you have not yet imported device administrators for that device. This message automatically appear after you perform the following operations:

- Adjust the ScreenOS version (changing the device firmware from ScreenOS 4.x to ScreenOS 5.x)—For details, see “Managing Device Firmware Version” on page 416.
- Upgrade to NetScreen-Security Manager FP2—For details, refer to the NetScreen-Security Manager FP2 Installer Guide.

To import device administrator information, from the file menu, select Devices > Configuration > Import Admins.

Configuring Authentication Servers

To authenticate device administrators when they attempt to connect to the security device, you can use the default authentication server (on the device), or an external authentication server.

The root device administrator is always stored and authenticated using the local database; however, for non-root read/write and read-only device admins (including vsys device admins), you can specify an external auth server (RADIUS, SecurID, or LDAP server) that stores device administrator accounts. To select an external server from the auth server list, you must have already created and configured an Authentication Server object in the NetScreen-Security Manager UI (for details, see “Configuring Authentication Servers” on page 502).

After the device administrator is authenticated, the auth server checks the privilege level of the device admin. A privilege level defines the privileges that are accessible to the device admin after successful logging in to the device:
For device administrators stored in the local database, the security device uses the privilege level specified in the local device administrator account.

For device administrators stored on an external auth server, select one of the following privilege settings:

- Get privilege from RADIUS server—Select this option to query a RADIUS server for all external device administrator privileges. The RADIUS server must contain the device administrator accounts and the netscreen.dct (Juniper Networks dictionary file).

- Read-Write, Read-Only—Select a privilege level that applies to all external device administrators. Although the device administrator accounts are stored on the external server, the security device provides the device administrator privilege level. Use this option when storing accounts on a SecurID or LDAP server, or when using a RADIUS server that does not contain the Juniper Networks dictionary file. By default, the external device administrator privilege level is set to Read-Only.

Configuring Device Administrator Accounts
You must create an account for each device administrator on the managed device. The device administrator account contains a device admin privilege level, user name, password, and optional PKA keys for the admin.

Additionally, for security devices that run ScreenOS 5.0 dial, you can configure privileges for the Trustee, such as granting the permission to configure the untrust Ethernet interface and the permission to configure the untrust modem interface.

Configuring Privilege Level
A security device supports multiple device administrators. NetScreen-Security Manager connects to the device as the root device administrator, and has complete administrative privileges for the device.

A security device can have only one root device administrator, which cannot be deleted. Additionally, after you create the root device administrator (or import from an existing device) you cannot change the name of the root device administrator. To delete an existing root device administrator, you can change the privilege level of the administrator to a non-root privilege, then save and delete the administrator. If you delete the root device administrator, however, you must then create a new root device administrator before installing the modeled configuration on the managed device (NetScreen-Security Manager must use the root device administrator account to communicate with the managed device).

**NOTE:** For ScreenOS 4.x devices, you can set or change the root device admin password using the directive “Set Root Admin”. To execute this directive, right-click the device in the Device Manager device list and select Device > Set Root Admin.

When you create other device administrators, you must assign a privilege level; these privileges are accessible to the device admin after successful login to the device:
Read/Write Device Administrator—The read/write administrator has the same privileges as the root device administrator, but cannot create, modify, or remove other device administrators. Privileges include:

- Creates virtual systems and assigns virtual system administrators
- Monitors any virtual system
- Tracks statistics (this privilege cannot be delegated to a virtual system administrator)

Read-Only Device Administrator—The read-only device administrator has only viewing privileges using the WebUI, and can only issue the `get` and `ping` CLI commands. Privileges include:

- Read-only privileges in the root system, using the following four commands: `enter`, `exit`, `get`, and `ping`
- Read-only privileges in virtual systems

Virtual System Device Administrator (available on security devices that support virtual systems)—Each virtual system (vsys) is a unique security domain, which can be managed by virtual system device administrators with privileges that apply only to that vsys. Virtual system administrators independently manage virtual systems through the CLI or WebUI. Privileges include:

- Creates and edits auth, IKE, L2TP, XAuth, and Manual Key users
- Creates and edits services
- Creates and edits policies
- Creates and edits addresses
- Creates and edits VPNs
- Modifies the virtual system administrator login password
- Creates and manages security zones
- Adds and removes virtual system read-only administrators

Virtual System Read-Only Device Administrator (available on security devices that support virtual systems)—A virtual system read-only administrator has the same set of privileges as a read-only administrator, but only within a specific virtual system. A virtual system read-only administrator has viewing privileges for a particular vsys through the WebUI, and can only issue the `enter`, `exit`, `get`, and `ping` CLI commands within that vsys.

For any configuration change made by a device administrator, the managed device generates a log entry with the name of the device administrator making the change, the IP address from which the change was made, and the time of the change. These log entries appear as configuration logs in the NetScreen-Security Manager Log Viewer.
Configuring Authentication

A device administrator can authenticate a connection to a security device using one of two authentication methods: Password or Public Key (ScreenOS 5.x devices only). However, regardless of the authentication method you want the device administrator to use, you must initially define a password for the admin account. If you later bind a public key to the admin, the password becomes irrelevant.

Use password authentication for device administrators who need to configure or monitor the managed device. You can use this authentication method for device administrators on ScreenOS 4.x and 5.x devices.

**NOTE:** All passwords handled by NetScreen-Security Manager are case-sensitive.

- To configure, enter a user name, password, and privilege level for the device administrator account, then select SSH Password Authentication.

- To connect using an SSH-aware application, the device administrator (the SSH client) initiates an SSH connection to the managed device (the SSH server). When SSH is enabled on the interface receiving the connection request, the managed device prompts the admin for user name and password, then compares that information to the information in the device admin account. If the user name and passwords match, the device authenticates the connection; if they do not match, the device rejects the connection request.

Use Public Key Authentication (PKA) for greater security, or to run automated scripts. You can use this authentication method for device administrators on a ScreenOS 5.x device.

- To configure, generate the PKA public/private key pair using the key generate program in an SSH client application (see the SSH client application documentation for more information). The key pair is RSA for SSHv1 and DSA for SSHv2. Assign the private key to the device administrator account, then load the public key on the managed device using a TFTP server or SSP (ScreenOS 5.1 and higher only).

- To connect using an SSH-aware application, the device administrator (the SSH client) initiates an SSH connection to the managed device (the SSH server). When SSH is enabled on the interface receiving the connection request, the managed device prompts the admin for user name and public key (of a public/private key pair), then compares that information with up to four public keys for that device admin account. If one of the keys matches, the device authenticates the connection; if no keys match, the device rejects the connection request.

When the managed device receives the connection request, it first checks the device administrator account for a public key bound to that administrator. If a matching key is found, the managed device authenticates the administrator using PKA; if no matching key is found, the managed device prompts for a user name and password. You can store up to four PKA keys for each device administrator.

You must enable SSH on the interface through which the device administrator connects to the managed device using an SSH connection.
Configuring Admin Accounts for Dialup Connections

The NS-5XT and the NS-5GT devices support a modem connection for outbound dial-up disaster recovery situations. You can set up trustee accounts for the interface or for the modem. This section describes the two types of trustees:

- **Interface trustee**
  
  An interface trustee has access only to the Untrust interface through the WebUI. An interface trustee can configure only assign the IP address for the primary Untrust zone interface. Also, an interface trustee accounts can enable or disable ping responses from an interface. Interface trustees can select either a PPPoE or DHCP client using automatic IP address assignment or a static address assignment client.

- **Modem trustee**
  
  A modem trustee can access, configure, and modify only the ISP1 and ISP2 settings. A modem trustee can also test and view the configurations for the ISP3 and ISP4 settings.

You can configure Modem Trustee and Interface Trustee accounts to have Read/Write or Read-Only levels of access.

The connection type to a device by a Trustee administrative account occurs exclusively, preventing any other connection type from occurring. The secure trustee connection prevents local console, Telnet, and SSH sessions to connect to the device if these other connection types attempt to use the trustee’s name or password.

In the following example, you configure a Read/Write modem trustee account for Richard Brockie. You set his user name to be rbrockie and his password to be !23fb.

**Configuring Permitted IPs**

Use permitted IPs to restrict management connections (a connection in which a device administrator attempts to log in) to specific IP addresses. By default, any host on the trust interface of the managed device can connect to the security device and attempt to log in. You can configure the device to permit management connections from one or more user-defined IP addresses only.

After you create Permitted IPs (and update the device with the modeled configuration), the device immediately begins rejecting management connections from non-permitted IP addresses. If a device administrator is managing the device using a remote network connection and the workstation is not included as a permitted IP, the security device immediately terminates the device administrator’s session.

To create a Permitted IP, click the Add icon in the Permitted IP area, then configure an IP address and netmask.

**NOTE:** Configuring a permitted IP for a device administrator does not affect the NetScreen-Security Manager – managed device connection.
EXAMPLE: CONFIGURING PERMITTED IPS
Corporation A has a small network, in which a single device administrator at 172.16.40.42 is allowed to manage the security device. For this device, you create a permitted IP with an IP/Netmask of 172.16.41.42/32.

Corporation B has a large network with multiple devices. Several device administrators on the 172.16.40.0 subnet require access to all devices. For each device, you create a permitted IP with an IP/Netmask of 172.16.40.0/24.

Configuring CLI Management
Use the CLI management options to configure local access using a console connection, or remote access using Telnet or SSH. A device administrator can connect directly to most security devices using the console port. CLI management settings apply to all device administrators for the security device.

Additionally, to manage a device remotely using Telnet or SSH, the device administrator must use a permitted IP address to initiate a Telnet or SSH connection to the device, and the correct service option must be enabled for the interface that the device administrator connects to on the device. For details on configuring permitted IP addresses, see “Configuring Permitted IPs” on page 304; for details on configuring service options for a device interface, see “Configuring Interface Service Options” on page 228.

Configuring the File Format
The file format determines the format (dos or unix) of a device configuration files. The CLI commands that configure the security device are automatically stored in a text-based configuration file. Occasionally, for troubleshooting purposes, a device administrator might need to view this configuration file outside of the security device.

To configure the file format of the configuration file, select the format that matches the computer system on which the configuration files will be viewed:

- In a UNIX text file, a line of text is terminated by a line feed character. When viewing a UNIX text file on a UNIX or DOS-based system, this line feed character does not appear. If you typically view configuration files on a UNIX system, select UNIX as the file format.

- In a DOS text file, a line of text is terminated by a line feed and a carriage return (\^M). When viewing a DOS text file on a UNIX system, the carriage return character appears onscreen. If you typically view configuration files on a DOS-based system, select DOS as the file format.

Configuring SSH and Telnet Ports
You can configure the port numbers to use for SSH and Telnet connections:

- The default port for SSH client connections is 22; to change this default, enter a port number between 1024 and 32767.

- The default port for Telnet client connections is 23; to change this default, enter a port number between 1024 and 32767.
In a vsys system, the root and vsys share the same SSH port number. For example, if you change the SSH port from the default port 22, the port is also changed for all vsys.

**NOTE:** For ScreenOS 4.x devices, you can set or change the device port numbers that accept Telnet and/or SSH connections. “Set Admin Ports”. To execute this directive, right-click the device in the Device Manager device list and select Device > Set Admin Ports.

### Configuring Connection Attempts

To minimize unauthorized access, you can limit the number of unsuccessful login attempts allowed before the security device terminates a Telnet session. This restriction also protects against certain types of attacks, such as automated dictionary attacks.

By default, a security device allows up to three unsuccessful login attempts before it closes the Telnet session.

### Configuring Password Length Restriction

To prevent a root device administrator from using short passwords (which are easier to decode and discover), you can set the minimum length requirement for the root device administrator password to any number from 1 to 31.

However, to set this restriction, the current root device administrator password must meet the minimum length requirement you are attempting to set. If the current password is too short, NetScreen-Security Manager displays an error message.

### Configuring Asset Recovery and Reset Hardware

If the root device administrator password is lost, the device administrator can restore access in one of two ways:

- **Using Asset Recovery**—Using a console connection, the device administrator uses the `unset all` command to clear all existing configuration settings and return the device to factory defaults (for details, see the “Administration” volume in the NetScreen Concepts & Examples ScreenOS Reference Guide). Device recovery is enabled by default. To disable it, clear the checkbox next to Enable Asset Recovery in the CLI Management configuration screen.

**NOTE:** A security device in FIPS mode automatically disables asset recovery.

- **Reset Hardware**—The device administrator performs a manual operation on the physical device hardware to return the device to factory defaults (for details, see the “Administration” volume in the NetScreen Concepts & Examples ScreenOS Reference Guide). Reset Hardware is enabled by default. To disable it, clear the checkbox next to Enable Reset Hardware in the CLI Management configuration screen.
All configuration settings stored on the managed device are lost during an asset recovery or hardware reset. After restoring access to the device, the device administrator should perform the following tasks to enable the device to reconnect to NetScreen-Security Manager:

1. Configure the interface that connects to the management system

2. Send the new root device administrator user name and password to the NetScreen-Security Manager administrator, who should update the existing root user name and password for the device in the modeled configuration.

3. Enable the NetScreen-Security Manager agent on the managed device.

After the device has re-connected to the management system, you (the NetScreen-Security Manager administrator) can update the device with the modeled configuration.

Configuring Console-Only Connections

You can require the root device administrator to log in to the security device through the console port only. This restriction requires the root device admin to have physical access to the device to log in, preventing unauthorized persons from logging in remotely.

By default, this restriction is not enabled (the root device administrator can log in remotely). To restrict access to console only, select the checkbox next to Root Access Console Only in the CLI Management screen. When enabled, the managed device denies access to all WebUI, Telnet, or SSH connections for the root device administrator. This setting overrides the management options enabled on the ingress interface.

Enabling the console-only setting does not affect the NetScreen-Security Manager-managed device connection.

Configuring SSH

Each security device includes a built-in Secure Shell (SSH) server. Device administrators can use an SSH-aware application to open a remote command shell on the device and execute commands. When using SSH, the connection is protected against IP or DNS spoofing attacks, and password or data interception.

The maximum number of SSH sessions is a device-wide limit and is between 2 and 24, depending upon the device. If the maximum number of SSH clients are already logged into the device, no other SSH client can log in to the SSH server.
To enable SSH connections to the managed device, select SSH Enable and configure an SSH Version. Because SSHv1 and SSHv2 are incompatible, you must use the same SSH version for both the client and server. For example, you cannot use an SSHv1 client to connect to an SSHv2 server on the managed device, or vice versa.

For the SSH server (the security device), you can also enable Secure Copy (SCP). A device administrator can use SCP to transfer files to or from the managed device using SSH (SSH authenticates, encrypts, and ensures data integrity for the SCP connection). When using SCP, the security device acts as an SCP server that accepts connections from SCP clients on remote hosts. Additionally, you must enable SSH for the managed device before you can enable SCP (disabled by default).

**NOTE:** For ScreenOS 4.x devices, you can enable or disable SSH for device admin connections using the directive “Set Admin SSH”. To execute this directive, right-click the device in the Device Manager device list and select Device > Set Admin SSH.

### Using SSH Version 1 (SSHv1)

SSHv1 is widely deployed and is commonly used. You can use a password or Public Key Authentication (PKA) to authenticate an SSHv1 connection.

When using PKA authentication for the SSHv1 server (the security device) you can also set the key generation interval for the host PKA key. When you enable SSH on a managed device, the device generates a unique host key that is permanently bound to the device (each vsys has its own host key). If SSH is disabled, then enabled again, the device uses the same host key. The security device uses the host key to identify itself to an SSH client (device administrator).

After the key is generated, it can be distributed to the SSH client in one of two ways:

- **Manually**—Send the host key to the client admin user via e-mail or phone. The device administrator stores the host key in the appropriate SSH file on the SSH client system (the SSH client application determines the file location and format).

- **Automatically**—When the SSH client connects to the managed device, the SSH server sends the unencrypted public component of the host key to the client. The SSH client searches its local host key database to see if the received host key is mapped to the address of the security device. If the host key is unknown (there is no mapping to the device address in the client’s host key database), the device admin user can accept the host key and authenticate the connection, or reject the host key and terminate the connection request.

To configure the SSH client, you must also bind the RSA PKA keys to the device administrator before that admin can make an SSH connection. For details on assigning PKA keys to a device admin, see “Configuring Device Administrator Accounts” on page 301.

**NOTE:** NetScreen-Security Manager supports PKA keys for device administrator authentication only for devices running ScreenOS 5.x.
Using SSH Version 2 (SSHv2)

SSHv2 is considered more secure than SSHv1 and is currently being developed as
the IETF standard.

To configure the SSH client, you must also bind the DSA PKA keys to the device
administrator before that admin can make an SSH connection. For details on
assigning PKA keys to a device admin, see “Configuring Device Administrator
Accounts” on page 301.

Configuring CLI Banners

You can customize the message that appears when a device administrator logs on
to the security device using a console connection, Telnet, or SSH. This message,
called a banner, provides confirmation to device administrators to let them know
that they have successfully logged in. Banners are optional; you are not required to
configure CLI banners for the security device.

A default banner already exists for Telnet and SSH, but you can write a new
message to suit your needs. You can use one banner for console connection and a
different banner for both Telnet and SSH connections.

To configure CLI banners:

- For console connections, enter a message in Console Login Banner text field.
  By default, the console banner is blank (no confirmation is provided to the
device administrator upon successful login). The maximum number of
  characters permitted in a console banner is 127.

- For Telnet or SSH connections, enter a new message or edit the existing default
  message in the Telnet/SSH Login Banner text field. By default, the message
  “Remote Management Console” is provided to device administrators upon
  successful login. The maximum number of characters permitted in a Telnet or
  SSH banner is 127.

For ScreenOS 5.1 and higher devices, you can also configure a secondary banner
for console, Telnet, or SSH connections. The secondary banner enables you to
create a much longer message that appears for any successful CLI-based connection
attempt. By default, the secondary banner is blank (no secondary message is
provided for device administrators upon login).

Configuring Web Management

Use the Web management options to configure remote access using Hypertext
Transfer Protocol (HTTP). A device administrator can use a standard Web browser
and HTTP to remotely access the WebUI on the security device. Web management
settings apply to all device administrators for the security device.

Additionally, to manage a device using the WebUI, the device administrator must
use a permitted IP address to initiate an HTTP connection to the device, and the
correct service option must be enabled for the interface that the device
administrator connects to on the device. For details on configuring permitted IP
addresses, see “Configuring Permitted IPs” on page 304; for details on configuring
service options for a device interface, see “Configuring Interface Service Options”
on page 228.
Configuring HTTP

You can configure the following options for administrative connections that use HTTP:

- Idle time for WebUI management—The number of seconds that the HTTP connection remains idle (no traffic is flowing) before the device drops the connection.

- Port number—The default HTTP port number is 80. If you are running HTTP services on a different device port, enter that port number here.

Additionally, the device administrator must use a permitted IP address to initiate an HTTP connection to the device, and the Web service option must be enabled for the interface that the device administrator connects to on the device.

To secure HTTP administrative traffic, you can use the Secure Sockets Layer (SSL) protocol.

Configuring SSL

Secure Sockets Layer (SSL) is a set of protocols that can provide a secure connection between a Web client and a Web server communicating over a TCP/IP network. SSL consists of the SSL Handshake Protocol (SSLP), which enables a client and server to authenticate each other and negotiate an encryption method, and the SSL Record Protocol (SSLRP), which provides basic security services to higher-level protocols such as HTTP. Using certificates, SSL authenticates the server (the security device), then encrypts the traffic sent during the session. Juniper Networks supports authentication only of the server (the security device), not the client (the device administrator); the device authenticates itself to the device administrator, but the device administrator does not use SSL to authenticate to the device. However, the device administrator must connect using a Web browser with SSL version 3 compatibility (not version 2). Netscape Communicator 4.7x and later and Internet Explorer 5.x later are SSL version 3 compatible.

During the SSL handshake, the security device sends the device administrator its self-signed certificate. The device admin encrypts a random number with the public key contained in the certificate and sends the number back to the device, which uses its private key to decrypt the number. Both participants then use the shared random number and a negotiated secret key cipher (3DES, DES, RC4, or RC4-40) to create a shared secret key, which they use to encrypt traffic between themselves. They also use an agreed-upon compression method (PKZip or gzip) to compress data and an agreed-upon hash algorithm (SHA-1 or MD-5) to generate a hash of the data to provide message integrity.

Additionally, the device administrator must use a permitted IP address to initiate an HTTP connection to the device, and the SSL service option must be enabled for the interface that the device administrator connects to on the device.

By default, SSL is disabled. To ensure that all HTTP connections to the WebUI are secure, you should enable this option. When enabled, the device automatically redirects administrative traffic using HTTP (default port 80) to HTTPs (SSL, default port 443) and authenticates using the local certificate. For device running ScreenOS 5.1 and higher, SSL uses the autogenerated, self-signed certificate on the device.
You can change the SSL configuration by editing the following SSL settings:

- Redirect HTTP to HTTPS—You can enable HTTP redirection for SSL troubleshooting, if desired.
- Certificate—By default, the security device uses an auto-generated self-signed certificate for SSL. To change the certificate used for SSL, select a certificate from the list of available certificates.
- Port—The default port for SSL connections is 443; to change this default, enter a different port number.
- Cipher—Select an encryption algorithm for SSL:
  - RC4-40 with 40-bit keys
  - RC4 with 128-bit keys
  - DES: Data Encryption Standard with 56-bit keys
  - 3DES: Triple DES with 168-bit keys
  The RC4 algorithms are paired with MD5; DES and 3DES with SHA-1.
- Authentication—Select an authentication method for SSL:
  - Message Digest version 5 (MD5)—128-bit keys
  - Secure Hash Algorithm version 1 (SHA-1)—160-bit keys

While SSL is enabled, any device administrator can connect to the security device using the SSL port. When administrative connections use SSL, in the Web browser URL field, the device admin must enter the https (instead of http) before the IP address used to manage the device. If you changed the default SSL port from 443, the device administrator must also append a colon and the SSL port number to the IP address. For example, to connect to the 5.5.5.5 interface and SSL port 1443, the device administrator must enter https://5.5.5.5:1443.

To use HTTP without SSL, simply disable SSL by clearing the Enable SSL checkbox. The device no longer redirects HTTP connections to SSL, and no authentication occurs for the connection.

**Configuring Date and Time Settings**

Use the Date/Time option to configure date and time synchronization on security devices. The date and time setting on the device affects VPN tunnel setup and schedule objects used in active Security Policies.

You configure the device time in relation to GMT.

**Configuring Network Time Protocol (NTP)**

To ensure that the security device always maintains the right time, the device can use NTP (Network Time Protocol) to synchronize its system clock with that of an NTP server on the Internet.
To use NTP, first enable Network Time Protocol, then configure the following settings:

- **Synchronization**—You can configure the security device to perform this synchronization automatically at time intervals that you specify. By default, the synchronization interface is set to 10 minutes, with a 3 second maximum adjustment threshold. For details on how to immediately synchronize the device system clock with an NTP server, see Chapter 7, “Managing Devices”.

- **Authentication**—To secure NTP traffic, enable authentication. When using authentication, for each NTP server you configure on the security device, you must assign a unique Server Key ID and Preshare Key; the key id and preshare key serve to create an MD5 checksum, with which the device and the NTP server can authenticate NTP data. Select the authentication mode that the device uses when connecting to an NTP server:
  - **Required**. The device must include the authentication information—Server Key ID and MD5 checksum—in every packet it sends to a NTP server and must authenticate all NTP packets it receives from a NTP server. If authentication fails, the device denies NTP traffic from the NTP server.
  - **Preferred**. The device attempts to authenticate NTP traffic using the same methods as the Required options, but continues to send and receive NTP traffic if authentication fails.
  - **None** (default mode). Select this mode if you do not want to authenticate NTP packets.

- **NTP Servers**—You can configure up to three NTP servers (one primary and two backups) from which the security device can regularly update its system clock. If you enabled authentication by selecting the Required or Preferred authentication options, you must also provide a unique Server Key ID and Preshare Key for each NTP server that you configure.

### Configuring an NTP Backup Server

You can specify an individual interface as the source address to direct NTP (Network Time Protocol) requests from the device over a VPN tunnel to the primary NTP server or a backup server as necessary. Among other interface types, you can select a loopback interface to perform this function.

The security device sends NTP requests from a source interface and optionally uses an encrypted preshared key when sending NTP requests to the NTP server. The encrypted preshared key provides authentication.

### Configuring Authentication

The authentication screens contain the following device-wide authentication options you can configure on a security device:

- Configuring General Auth Settings
- Configuring Banners
The following sections detail each authentication option.

### Configuring General Auth Settings

For devices running ScreenOS 5.2, you can configure some general settings that determine how the security device handles authentication session cleanup and authentication requests.

#### Clearing RADIUS Sessions

Occasionally, overcharging can occur when a wireless user is assigned the same IP address as was used for a previously closed connection by a different user. Because the IP addresses are the same for both connections, the first wireless user might be charged for the second user’s connection time. You can prevent this problem by configuring the security device to clear RADIUS sessions for a specific IP address when the RADIUS accounting-stop message is received for that connection.

To enable session cleanup for a security device, in the device navigation tree, select Auth > General. Configure a RADIUS Accounting Listener port that monitors the connection for accounting-stop messages, then select the option RADIUS Accounting Cleanup Action: Session Cleanup.

#### Assigning an Authentication Request Interface

By default, the security device sends authentication requests using the route defined in the route table. For devices running ScreenOS 5.2, you can configure a specific outgoing source interface for requests sent to an authentication server. You might need to specify a specific interface for auth requests destined for a VPN tunnel, or simply to route all auth requests through the same interface for authentication monitoring.

To configure a source interface, in the device navigation tree, select Auth > General, then click the Add icon in the Source Interface used for Outgoing Auth Request area. Select the Authentication Server object that represents the authentication server receiving the request, then select an interface on the device through which requests are sent.

---

**NOTE:** For details on configuring Authentication Server object, see “Configuring Authentication Servers” on page 502.

---

After you specify a source interface for auth requests, the security device routes all auth requests destined for a RADIUS, LDAP, or SecurID server through that interface (one source interface per authentication server object).
Configuring Banners

You can customize the message that appears when a device administrator logs on to the security device Telnet, FTP, HTTP, or via WebAuth. This message, called a banner, provides confirmation to device administrators to let them know the status of the connection. Default banners already exist, but you can write a new message to suit your needs. You can use different banners for each protocol.

NOTE: To configure the Telnet, SSH, or console connection banner, see “Configuring CLI Banners” on page 309.

To configure a protocol banner, select the protocol tab and edit the default Telnet, FTP, and HTTP messages:

- Attempted Logins—Enter a new message or edit the existing default message in the Login text field. This message is provided to device administrators when they are prompted for their authentication credentials.

- Successful Logins—Enter a new message or edit the existing default message in the Success text field. This message is provided to device administrators after their credentials have been authenticated and a connection has been established.

- Failed Logins—Enter a new message or edit the existing default message in the Fail text field. This message is provided to device administrators when their credentials are not authenticated (authentication fails) or when the administrator is not authorized to access the device.

To configure the WebAuth banner, select the WebAuth tab and enter a new message (or edit the existing default message in the Success text field. This message is provided to auth user when their WebAuth credentials have been authenticated and a connection has been established. The message appears at the top of a Web browser screen, after an auth user has successfully logged on to a WebAuth address. Typically, the message simply informs the user that the authentication was successful, but you can enter any message you want, up to a maximum of 220 characters.

Banners are optional; you are not required to configure banners for the security device.

Configuring Default Servers

The default servers for the security device define the authentication servers used to provide local, external, and WebAuth user authentication.

The Local server is the security device itself. All security devices support a built-in database for authentication; this database is the default server (authentication server) for all types of authentication that occur on the device. The user names and authentication credentials of all local users are stored in this local database.
Alternatively, you can select an external authentication server as the default server. To select an external server, you must have already created and configured an Authentication Server object in the NetScreen-Security Manager UI. You must also have defined the user accounts for all external users on the external server. For details, see “Configuring Authentication Servers” on page 502 and “Configuring User Objects” on page 511.

For the Local server only, you can set the authentication timeout, which is the number of minutes the connection remains active after an authentication request has been submitted and a successful authentication is received. By default, the authentication timeout on the Local authentication server is 10 minutes. To change this timeout, enter a new value.

Configuring an Auth Server
The default Auth Server for a device handles all types of authentication that occur on the device, including user authentication. Select the Local authentication server to provide authentication for local users defined in the local database.

Configuring a WebAuth Server
When using WebAuth, an auth user first initiates an HTTP session to the IP address on the security device that hosts WebAuth. After successfully authenticating, the auth user can send traffic to the destination (as permitted by the Security Policy). To authenticate WebAuth users, you can use the Local authentication server (on the security device), or select a previously-defined external auth server.

Configuring Infranet Settings
If you have deployed Juniper Networks’ Infranet Controllers as part of your network security infrastructure, you can use the Infranet Settings screen on devices running ScreenOS 5.3 and above to configure the following properties:

- Contact Interval—this setting determines the time interval (in seconds) that the Infranet Enforcer waits before attempting to connect to the next available Infranet Controller; the default interval is set to 10 seconds.

- Action on Timeout—if for any reason your connection to the Infranet Controller times out, the device terminates the SSH connection and clears all Infranet Controller related context. You can change this behavior by setting the timeout action to “Open”, in which case the Infranet Enforcer allows all traffic; or “No Change”, in which case the Infranet Enforcer preserves the current state of all existing tunnel sessions.

- Enforcer Mode—use this setting to take the Infranet Enforcer out of regular mode and into “Test” mode. “Test” mode is recommended before you actually deploy the Infranet Enforcer enabling you to evaluate how the solution works. In this mode, the Infranet Enforcer allows all traffic that matches the Infranet policy. Logs are created indicating the behavior of the Infranet Enforcer as if it were operating in “Regular” mode.

- Infranet Controllers—you can configure up to eight (8) Infranet Controllers. The order in which these are entered is used by the Infranet Enforcer to contact each Infranet Controller.
You can also configure security devices to authenticate using Infranet Controllers in a rule in a Security Policy. Refer to “Configuring Authentication For Firewall Rules” on page 553 for more information.

Configuring Reporting

The Report Settings screens contain reporting options that you can set for the device. In the Device dialog box, open the Report Settings heading to see configuration options.

This section provides an overview of the following reporting options for security devices. For details on configuring reporting settings, “Configuring the Device for Logging” on page 728.

For more detailed explanation about reporting concepts for the security devices, see the “Administration” volume in the NetScreen Concepts & Examples ScreenOS Reference Guide.

Configuring General Reporting Settings

Use the General reporting settings to configure the severity levels of the messages you want to log and where you want those messages sent. Each system event on a security device is assigned a level of severity. You can configure your security device to send messages to specific destinations to communicate events of a certain level of severity. By default, packets that are dropped on the security device are logged to the self log. In the Firewall Options, you can disable or enable logging of dropped packets for specific traffic types, including ICMP, IKE, SNMP, and multicast packets.

You can also use this tab to set thresholds determining how many packets of a particular type the Packet Process Unit (PPU) sends to the CPU per second, before dropping subsequent packets of that type. The PPU is a hardware processor in some NetScreen systems that forwards packets to the flow CPU. Enabling PPU packet drop thresholds adds an extra layer of DoS-attack protection to the device, similar to SYN-cookie and SYN-proxy. In effect, PPU protection prevents DoS attacks from overwhelming the flow CPU, thus keeping the CPU responsive to critical tasks even under heavy traffic. PPU protection processes three categories of traffic: Packets that do not use the IP protocol; Packets carrying contents other than TCP or UDP; and System-critical IP packets, including BGP, OSPF, RIP, SNMP, system management, SIP, and H323 traffic.

For details on configuring General reporting options, see “Configuring the Device for Logging” on page 728.

Configuring Email Notification Settings

Use the Email option to configure a security device to send messages using email whenever a system event of Emergency, Alert, Critical, or Notification severity level occurs. To configure email notification, you must specify the SMTP mail server and at least one email address; if desired, you can enter a secondary email address as well.

For details on configuring Email reporting options, see “Configuring Email Server Settings” on page 730.
Configuring NetScreen-Security Manager Reporting

Use the NetScreen-Security Manager reporting settings to configure the security device to report specified events to NetScreen-Security Manager. You configure the primary IP address of the NetScreen-Security Manager Device Server and select the categories of events that are tracked on the security device and reported to NetScreen-Security Manager. You can also set the interval at which the NetScreen-Security Manager Device Server polls for policy statistics and protocol distribution events.

For details on configuring the NetScreen-Security Manager reporting options, see “Configuring Events Reporting Settings” on page 730.

Configuring SNMP Reporting

Use the SNMP reporting options to configure the Simple Network Management Protocol (SNMP) agent for the security device. The SNMP agent provides a view of statistical data about the network and the devices on it, and notification of system events of interest.

You also must enable SNMP manageability on the interface through which the SNMP manager applicable communicates with the SNMP agent in the security device.

For details on configuring SNMP reporting options, see “Configuring SNMP Reporting Settings” on page 736.

Configuring Syslog Reporting

Use the Syslog option to configure syslog reporting. A security device can generate syslog messages for system events at predefined severity levels and optionally for traffic that policies permit across a firewall. It sends these messages via UDP (port 514) to up to four designated syslog hosts running on UNIX/Linux systems. When you enable syslog reporting, you also specify which interface the security devices uses to send syslog packets.

Configuring a Syslog Host

To configure a syslog host:

1. Click the Add icon in the Syslog configuration screen. The host configuration dialog box appears.

2. Specify the hostname and the port to which the security device sends syslog messages.

3. For each syslog host, you specify the following:

   - Whether the security device includes traffic log entries, event log entries or both traffic and event log entries
   - The security facility, which classifies and sends messages to the Syslog host for security-related actions; and the regular facility, which classifies and sends messages for events unrelated to security
Which transport protocol (UDP or TCP) is used for sending syslog messages?

4. Click OK.

For details on configuring syslog reporting options, see “Directing Logs to a Syslog Server” on page 737.

Configuring Webtrends Reporting

Use the Webtrends option to configure the security device to send syslog reports to a Webtrends Syslog host. Webtrends offers a product called the Webtrends Firewall Suite that enables you to customize syslog reports to display the information you want in a graphical format.

To configure the security device to send syslog reports to a Webtrends Syslog host, you first enable Webtrends reporting, then specify the name of the Webtrends host and the port on which the syslog message are sent. If you are sending reports through a VPN tunnel, click the Use Trust Zone Interface as Source IP for VPN check box.

For details on configuring Webtrends reporting options, see “Directing Data to a WebTrends Server” on page 738.

Configuring Security

The Security screens contain security options that you can set for the device. In the Device dialog box, open the Security heading to see configuration options.

This section describes configuring the following security options for security devices:

- Configuring AntiVirus (AV) Settings
- Configuring Antispam
- Configuring Web Filtering
- Configuring Deep Inspection
- Configuring the Attack Database
- Disabling Attack Objects
- Configuring Security Module (SM) Settings

Configuring AntiVirus (AV) Settings

(This option is only available on some security devices.) Use the antivirus (AV) option to configure AV scanning. Security devices provide two antivirus scanning methods:
External AV scanning—This method uses a Trend Micro device for scanning. (This option is supported by devices running ScreenOS 5.2. Not supported in ScreenOS 5.3.) The security device forwards all traffic to be scanned to the Trend Micro device. To configure external AV scanning, use the AV Scanner settings (detailed below).

Internal AV scanning—This method uses the AV scanner on the security device, and is not supported by all security devices. To configure internal AV scanning, use the AV Scan Manager settings (as detailed on page 320).

You can also configure the internal AV scanner to scan webmail responses from a Web server to a client. For details, see “Configuring AV HTTP Webmail Settings” on page 321.

Configuring External AV Scanners
Use the AV Scanner Settings tab to configure the following:

- Fail Mode Traffic Permit—When enabled, the security device continues to permit traffic even if the device loses connectivity with the AV scanner.

- Maximum AV resources allowed per AV client—Determines the maximum percentage of AV resources that an AV client can consume. The default is 70%; acceptable range is 1% to 100%, where 100% allows unrestricted resource consumption. You might want to edit this option to prevent a malicious user from generating a large amount of traffic in an attempt to consume all available resources.

HTTP Settings

- HTTP keep-alive—Directs the device to use the HTTP keep-alive connection option. Using this option prevents the device from sending a TCP FIN message to indicate termination of data transmission.

- Skip scanning HTTP content with predefined content type—By default this option is enabled. This means HTTP scanning does not scan HTTP entities composed of any of the following Multipurpose Internet Mail Extensions (MIME) content types (and when followed by a slash, subtypes):
  - application/x-director
  - application/pdf; image
  - video
  - audio
  - text/css
  - text/html

Because most HTTP entities are composed of these content types, HTTP scanning only applies to a small subset of HTTP entities such as /zip and application /exe content types, where viruses are most likely to be hiding.
- **Trickling**—You can direct the device to forward specific amounts of unscanned traffic to the HTTP client to prevent the client from timing out while the scanner is busy examining downloaded HTTP files. If you select Custom, you can specify the amounts that are forwarded. Selecting Default resets the amounts to their default values.

**Configuring the Internal AV Scanner**

Use the AV Scan Manager Settings tab to configure the following:

- **Pattern Server URL**—You specify the URL address of the server from which the device retrieves pattern file updates.

Use one of the following two default pattern-update URLs:

- To use the Kaspersky internal antivirus scanner
  
  http://update.juniper-updates.net/av/5gt

- To use the Trend Micro internal antivirus scanner
  
  http://5gt-p.activeupdate.trendmicro.com/activeupdate/server.ini

- **Update Interval**—You can specify the interval at which the device starts an automatic pattern update.

**NOTE:** You can direct a security device to immediately contact the pattern server and update its pattern file. To do this, right-click the device object and select AV Scan Manager > Update Pattern. (You can modify the pattern server URL and update interface if necessary.) Click OK.

- **Update type**—You can indicate whether you want to download the in-the-wild Virus and Spyware pack, the All Virus and Spyware pack, or the All Virus and Spyware, plus adware/pornware/riskware/greyware pack.

- **Maximum Decompression level**—You can specify the number of levels of compression to examine. A setting of 2 will examine a compressed file within a compressed file. If the number of levels of compression in the file exceeds the number indicated here, the email will be blocked.

- **Content drop parameters**—You can specify that the device drop messages if the size of the content or the number of concurrent messages exceed configurable limits.

- **Content Protocol**—You can select the type of protocols (HTTP, SMTP, FTP, IMAP or POP3) that are to be examined for virus patterns. For each protocol, you can also specify the following (not all values applicable to all protocols):

  - **Scan Mode**: All, Intelligent, or by File Extension. If you select Scan by File Extension, you must populate the Ext List Include field.

  - **Scanning Timeout**: scans that take longer than this time out and are not completed.
Decompress Layer: the number of levels of decompression to uncompress before scanning. A decompression setting of 2 would all the scanning of a .zip file withing a .zip file. Supported by ScreenOS 5.3 and higher. For ScreenOS 5.2 and lower, must be configured on an individual scanner basis.

Skip Mime (HTTP only): if checked, causes the scanner to skip any mime types listed in the Mime List field. Supported by ScreenOS 5.3 and higher. For ScreenOS 5.2 and lower, must be configured on an individual scanner basis.

Ext List Include: a list of file extensions to examine for viruses. Extension lists are created under Object Manager > AV Objects > Extension Lists.

Ext List Exclude: a list of file extensions to not examine for viruses. Extension lists are created under Object Manager > AV Objects > Extension Lists.

Mime List (HTTP only): the list of mime types to not scan. Netscreen-Security Manager ships with a default mime type list, or you can create your own under Object Manager > AV Objects > Custom Mime Lists.

Email Notify Virus Sender (IMAP, POP3, SMTP only): Notifies an email sender if a virus was found in the email.

Email Notify Scan-Error Sender (IMAP, POP3, SMTP only): Notifies an email sender if the email was dropped due to a scan error.

Email Notify Scan-Error Recipient (IMAP, POP3, SMTP only): Notifies an email recipient if the email was passed due to a scan error.

Configuring AV HTTP Webmail Settings
You can also configure the internal AV scanner to scan webmail responses from a Web server to a client. When a client makes an HTTP webmail request, the security device can intercept the Web Server response, scan the response for viruses, then forward to the client.

Because networks typically handle a large amount of HTTP traffic, you might want to enable scanning for WebMail only. When enabled, the internal AV scanner scans HTTP traffic for webmail only (non-webmail HTTP traffic is not scanned). When disabled, the device scans all HTTP traffic for viruses.

The internal AV scanner examines specific HTTP webmail patterns only (many popular providers are predefined). To configure Webmail scanning, you must define the URL parameters:

- URL Pattern—Specifies a URL pattern identifying a certain type of WebMail to examine for virus patterns. When the URL matches all of the following parameters, the AV scanner performs a virus scan.

- Path in URL—Specifies the download URL path for the webmail.
- Path Exclusion—Excludes the listed path from scans. Supported in ScreenOS 5.3 and higher.

- Argument in URL—Specifies the URL argument. Arguments begin with a question mark (?).

- Argument Exclusion—Excludes the listed argument from scans. Supported in ScreenOS 5.3 and higher.

- Host Name in URL—Specifies the host name in the URL.

- Host Exclusion—Excludes the listed host from scans. Supported in ScreenOS 5.3 and higher.

For more details on AV, see the “Attack Detection and Defense Mechanisms” volume in the NetScreen Concepts & Examples ScreenOS Reference Guide.

Configuring AV Scanner Settings

The third tab in the Device-specific or Template-specific AntiVirus settings is the AV Scanner Settings tab. Use this tab to configure the following settings for your device:

- **Fail Mode Traffic Permit**—Check this checkbox if you want the device to pass through unexamined traffic when it fails to contact the antivirus scanner. If you want the device to block unexamined traffic, leave the box unchecked.

- **Maximum AV resources allowed per AV client**—Sets the maximum percentage of device resources a single source can occupy at one time. Prevents one source from overwhelming the device.

- **HTTP keep alive**—Check this checkbox to keep the HTTP connection alive while antivirus scanning occurs.

- **Trickling**—“Trickling” is the act of forwarding some HTTP traffic to the requesting client so the browser doesn’t time out during the antivirus scan. Three settings are available:

Table 16: Trickling Settings

| Disable | Select this option to disable HTTP trickling. |
Chapter 5: Configuring Devices

Configuring Antispam

ScreenOS 5.3 supports antispam functionality.

Use Antispam to tag or block unwanted emails based on email ID, hostname, domain name, or IP address. SMTP is supported but not POP3 or IMAP. Advanced features such as Bayesian filtering are not supported. Requires ScreenOS 5.3 or higher.

Email is tagged or blocked based on lists. Blacklists and whitelists can be configured locally, and Juniper provides a server with a blacklist of known spammers. Netscreen-Security Manager first attempts to match each email against the local lists. If it does not match a local list, it then attempts to match the email against the list on the Juniper server.

Emails are tagged or blocked (depending on settings) if they match any parameter in one of the blacklists, unless they also match a parameter in the whitelist. The following table shows how the three lists interact:

<table>
<thead>
<tr>
<th>Local Whitelist</th>
<th>Local Blacklist</th>
<th>Juniper Blacklist</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Match</td>
<td>Match</td>
<td>Not Checked</td>
<td>No Action (allow through)</td>
</tr>
<tr>
<td>Match</td>
<td>No Match</td>
<td>Not Checked</td>
<td>No Action (allow through)</td>
</tr>
<tr>
<td>No Match</td>
<td>Match</td>
<td>Not Checked</td>
<td>Block or Tag</td>
</tr>
<tr>
<td>No Match</td>
<td>No Match</td>
<td>Match</td>
<td>Block or Tag</td>
</tr>
<tr>
<td>No Match</td>
<td>No Match</td>
<td>No Match</td>
<td>No Action (allow through)</td>
</tr>
</tbody>
</table>

To configure a security device for Antispam, you must turn on Antispam in a policy and configure antispam settings on a device.
Configuring Antispam Settings for a Device
1. Open a security device in Device Manager.
2. Select Security > Antispam.
3. Populate the listed fields:
   - Antispam Whitelist — Emails that contain email addresses, IP addresses, hostnames, or domain names in this list will always be accepted by the filter, even if the email also matches an entry in the blacklist.
   - Antispam Blacklist — Emails that contain email addresses, IP addresses, hostnames, and domain names in this list will be tagged or blocked, unless the email also contains a match in the whitelist.
   - Action for Spam — Indicates whether email that matches a blacklist entry will be tagged (and passed along) or blocked.
   - Tag Subject or Header — If blacklist emails are to be tagged, indicates whether the tag will be placed in the header or subject line of the email before it is passed on.
   - Tag String — If blacklist emails are to be tagged, indicates the character string that will be placed in the email.
   - Enable use default SBL server — If checked, compare emails that do not match the local blacklist or whitelist to the blacklist of known spammers on the Juniper server. If this checkbox is not checked, only the local lists will be used.

EXAMPLE: TURNING ON ANTISPAM IN A POLICY
1. Install an Antispam license key to enable the Antispam option on the security device. For details, see “Managing License Keys” on page 418. To check the status of the Antispam option for a device, open the device configuration and select Info > Capabilities. If the license has been installed, Antispam Profiles is enabled.
2. Open the policy my_antispam_policy.
3. Double-click the Rule Options cell in the desired rule row.
4. Select the Antispam tab in the Configure Options dialog box.
5. Check the Enable Antispam profile checkbox.
6. Select ns-profile from the Profile Name pull-down menu.
7. Click OK to close the Configure Options dialog.

EXAMPLE: CONFIGURING ANTISPAM IN A TEMPLATE
In this example, you configure the device put the string ***SPAM*** in the subject line of emails from wesendspam.com.
1. In the main navigation tree, select Device Manager > Security Device > Templates. Doubleclick a template to open it.

2. In the device navigation tree, select Security > Antispam.

3. Click the Add icon in the Antispam Blacklist area.

4. Type wesendspam.com in the Entry field and click OK.

5. In the Action for Spam field, select Tag Spam Email.

6. In the Tag Subject or Header field, select subject.

7. In the Tag String field, enter ***SPAM***.

8. Check the Enable use default SBL server checkbox.

9. Click OK to save your changes to the template.

Configuring Web Filtering

Use the Web Filtering option to manage Internet access and prevent access to inappropriate web content.

To configure a security device for Web filtering, you must perform the following steps:

1. Install a Web license key to enable the Web Filtering option on the security device. For details, see “Managing License Keys” on page 418. To check the status of the Web Filtering option for a device, open the device configuration and select Info > Capabilities. If the license has been installed, Web filtering (Integrated) is enabled.

2. Configure at least one Domain Name Server (DNS) so the security device can resolve the SurfControl CPA server name to an address. For details on configuring DNS, see “Configuring DNS Settings” on page 292.

3. Select a Web filtering method and configure the Web filtering settings on the security device. You can select one of the following Web filtering methods for each security device:
   - Integrated Web Filtering (SurfControl CPA)—Block or permit access to a requested website by binding a SurfControl-defined or custom Web filtering profile to a firewall rule for the security device. A Web filtering profile contains Web categories (list of predefined or custom URLs) and the action the security device takes (permit or block) when it receives a request to access a URL.
   - Redirect Web Filtering (SurfControl SCFP)—Block or permit access to different web sites based on SurfControl-defined URLs, domain names, and IP addresses.
   - Redirect Web Filtering (Websense)—Block or permit access to different web sites based on Websense-defined URLs, domain names, and IP addresses.
The following sections detail the Web filtering settings.

4. Define categories and profiles (optional); for details, see “Configuring Web Filtering Objects” on page 485.

5. Assign a Web filtering profile to a firewall rule; for details, see “Configuring WEB Filtering for Firewall Rules” on page 551.

Configuring Integrated Web Filtering
With integrated Web filtering, you can permit or block access to a requested website by binding a Web Filtering profile to a firewall rule. A Web Filtering profile contains Web Categories and the action the security device takes (permit or block) when it receives a request to access a URL.

A URL category is a list of URLs organized by content. SurfControl Content Portal Authority (CPA) servers maintain a large database of all types of web content classified into 40 categories. For a list of SurfControl Web Categories, see Appendix C, SurfControl URL Categories.

SurfControl has three server locations that each serve a specific geographic area: the Americas, Asia Pacific, and Europe/Middle East/Africa. The default primary server is the Americas; the default backup server is Asia Pacific.

URLs and categories created and maintained by SurfControl appear in the NetScreen-Security Manager UI as predefined, and cannot be edited. You can also create custom URLs, then use those URLs within a custom Web Filtering Profile. For details on viewing predefined Web Categories and configuring Web Filtering Profiles, see “Configuring Web Filtering Objects” on page 485.

EXAMPLE: CONFIGURING INTEGRATED WEB FILTERING
In this example, you select SurfControl CPA (Integrated) as your Web Filtering profile.

1. In the main navigation tree, select Device Manager > Security Devices, then double-click the device for which you want to configure Web Filtering. The device configuration appears.

2. In the device navigation tree, select Security > Web Filtering, then click the SurfControl CPA (Integrated) tab.

3. Select CPA Server Enable, then configure the following SurfControl Settings:
   - For Server, select America.
   - For Primary Host, enter usi.SurfCA.com.
   - For Primary Port, enter 9020.
   - For Fail Mode select block.

4. Select Enable Cache, then configure the following cache settings:
   - For Cache Timeout (hours), enter 24.
For Cache Size (K bytes), enter 500.
For Query Interval (weeks), enter 2.

5. Click OK to save your settings and close the device configuration.

Redirect Web Filtering
Redirect Web Filtering enables you to block or permit access to different web sites based on their URLs, domain names, and IP addresses. NetScreen-Security Manager supports redirect Web Filtering using either the Websense Enterprise Engine or SurfControl Web Filter.


For Websense, ScreenOS supports up to eight Web-filtering servers. On vsys devices, one server is reserved for the root, leaving seven servers available for vsys (one server per vsys, all remaining vsys must use root server). For vsys-capable devices running ScreenOS 5.2, you can assign the same server to multiple vsys devices, then configure a profile name for each vsys to enable the filtering server to distinguish between vsys devices.

Select the redirect Web Filtering method you want to use, enable Web Filtering for that method, then configure the settings:

- **Source Interface**—The source from which the security device initiates Web filter requests to a Web-filtering server.
- **Server Name**—The IP address or fully qualified domain name (FQDN) of the Websense or SurfControl server.
- **Server Port**—The port number on the filtering server that handles filtering requests. The default port for Websense is 15868; the default port for SurfControl is 15868.
- **Profile Name**—(vsys capable devices running ScreenOS 5.2 only) The profile name uniquely identifies the device when connecting to the filtering server. When configuring Websense (Redirect) Web-Filtering for multiple vsys devices using the same root device, you can assign the same Web-filtering server and port to multiple vsys devices as long as you use a unique profile name for each device.

NOTE: If you change the default port on the server you must also change it on the security device.

- **Profile Name**—(vsys capable devices running ScreenOS 5.2 only) The profile name uniquely identifies the device when connecting to the filtering server. When configuring Websense (Redirect) Web-Filtering for multiple vsys devices using the same root device, you can assign the same Web-filtering server and port to multiple vsys devices as long as you use a unique profile name for each device.

NOTE: All vsys devices assigned to the same WebSense Web-Filtering server use the same Server Timeout, Fail Mode, and Message Type. Although you can configure different values for these fields for different vsys devices in the NetScreen-Security Manager UI, the WebSense server uses only the values defined for the vsys device that most recently contacted the Web-Filtering server.
Configuring Security

Server Timeout—The time interval, in seconds, that the security device waits for a response from the Web-filtering server. If the server does not respond within the time interval, the security device either blocks the request or permits it. For the time interval, you can enter a number between 10 and 240.

Fail Mode—The fail mode (Block or Permit) determines how the security device handles HTTP requests if the device loses contact with the Web-filtering server.

Message Type—The source of the message the user receives when Websense or SurfControl blocks a site.

- If you select NetPartners Websense/SurfControl, the security device forwards the message it receives from the Websense or SurfControl server.
- If you select NetScreen, the security device sends the message that you entered in the Message Sent to Blocked Client field.

NOTE: If you select NetScreen, some of the functionality that Websense provides, such as redirection, is suppressed.

Message Sent to Blocked Client—This is the message the security device returns to the user after blocking a website. You can use the message sent from the Websense or SurfControl server, or create a message (up to 500 characters) to be sent from the security device.

EXAMPLE: CONFIGURING WEBSENSE REDIRECT WEB FILTERING
Select Websense (Redirect) as your Web Filtering policy.

1. In the main navigation tree, select Device Manager > Security Devices, then double-click the device for which you want to configure Web Filtering. The device configuration appears.

2. In the device navigation tree, select Security > Web Filtering, then click the Websense (Redirect) tab.

3. Select Enable Web Filtering, then configure the following WebSense settings:
   - For Source Interface, select untrust.
   - For Server Name, enter 10.1.2.5.
   - For Server Port, enter 15868.
   - For Server Timeout (sec), enter 10.
   - For Fail Mode, select Permit.
   - For Message Type, select NetScreen.
   - For Message Sent to Blocked Client, enter “We’re sorry, but the requested URL is prohibited. Contact ntwksec@mycompany.com”.

4. Click OK to save your settings and close the device configuration.
Configuring Deep Inspection

(This option is only available on some security devices.) Deep Inspection (DI) is a mechanism for filtering permitted traffic. When you enable Deep Inspection in a firewall rule, the device examines permitted traffic and takes action if the DI module in ScreenOS finds attack signatures or protocol anomalies.

The Juniper Security team provides multiple DI signature packs for different security needs. Packs are covered by license keys. You must get a license key to enable a signature pack. Only one signature pack can exist for a given device.

Available signature packs are as follows:

- Server Protection Pack
- Client Protection Pack
- Worm Mitigation Pack
- Base (Default) Pack

Use the Deep Inspection configuration screens to modify the default settings defined in RFCs and RFC extensions for the following protocols:

<table>
<thead>
<tr>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIM</td>
</tr>
<tr>
<td>IDENT</td>
</tr>
<tr>
<td>NTP</td>
</tr>
<tr>
<td>SNMP/Trap</td>
</tr>
<tr>
<td>CHARGEN</td>
</tr>
<tr>
<td>IKE</td>
</tr>
<tr>
<td>POP3</td>
</tr>
<tr>
<td>SQL Mon</td>
</tr>
<tr>
<td>DHCP</td>
</tr>
<tr>
<td>IMAP</td>
</tr>
<tr>
<td>PortMapper</td>
</tr>
<tr>
<td>SSH</td>
</tr>
<tr>
<td>DISCARD</td>
</tr>
<tr>
<td>IRC</td>
</tr>
<tr>
<td>RADIUS</td>
</tr>
<tr>
<td>SSL</td>
</tr>
<tr>
<td>DNS</td>
</tr>
<tr>
<td>LDAP</td>
</tr>
<tr>
<td>Rexec</td>
</tr>
<tr>
<td>Syslog</td>
</tr>
<tr>
<td>ECHO</td>
</tr>
<tr>
<td>LPR</td>
</tr>
<tr>
<td>rlogin</td>
</tr>
<tr>
<td>TELNET</td>
</tr>
<tr>
<td>FINGER</td>
</tr>
<tr>
<td>MSN</td>
</tr>
<tr>
<td>SunRPC</td>
</tr>
<tr>
<td>TFTP</td>
</tr>
<tr>
<td>FTP</td>
</tr>
<tr>
<td>MSRPC</td>
</tr>
<tr>
<td>Rsh</td>
</tr>
<tr>
<td>VNC</td>
</tr>
<tr>
<td>GNUTELLA</td>
</tr>
<tr>
<td>MS-SQL</td>
</tr>
<tr>
<td>RTSP</td>
</tr>
<tr>
<td>WHOIS</td>
</tr>
<tr>
<td>GOPHER</td>
</tr>
<tr>
<td>NBNAME</td>
</tr>
<tr>
<td>Rusers</td>
</tr>
<tr>
<td>Yahoo Messenger</td>
</tr>
<tr>
<td>HTTP</td>
</tr>
<tr>
<td>NFS</td>
</tr>
<tr>
<td>SMB</td>
</tr>
<tr>
<td>ICMP</td>
</tr>
<tr>
<td>NNTOP</td>
</tr>
<tr>
<td>SMTP</td>
</tr>
</tbody>
</table>
For details on each protocol and its settings, refer to the “di” command in the NetScreen CLI Reference Guide.


Configuring the Attack Database

(This option is only available on some security devices.) Use the Attack Database option to configure a database that contains all the predefined attack objects, organized into attack object groups by protocol and severity level.

Juniper Networks stores the attack object database on the attack object update server at https://services.netscreen.com/restricted/sigupdates. To gain access to the attack object update server, you must first obtain an attack object update subscription for your security device. To obtain a subscription for a device using the NetScreen-Security Manager UI, see “Activating Subscription Services” on page 419.

After you have obtained a subscription, you must update the attack object database on the GUI Server and managed device. The update process differs slightly between devices running ScreenOS 5.1 and higher and devices running 5.0; for details, see “Updating the Attack Object Database” on page 420.

For all devices, the attack object database on the managed device must match the version of the attack object database on the GUI Server. If the databases do not match, a validation icon appears next to the Attack Database Version setting, and the Disable Attack option does not appear in the device navigation tree.

To use the predefined attack objects, create a DI Profile object that references specific attack object groups and configure a firewall rule to use that profile object. For details on creating a DI Profile object, see

To configure the attack object database, specify the following:

- URL of the attack object database server. NetScreen-Security Manager downloads the latest version of the attack object database via the Internet, from https://services.netscreen.com/restricted/sigupdates.
  
  When you update the attack object database for a device running ScreenOS 5.0.x, the device connects to this URL and downloads the latest database version.

- When you update the attack object database for a device running ScreenOS 5.1 and higher, the management system automatically connects to the URL specified in the UI Preferences and downloads the new database version to the GUI Server. ScreenOS 5.1 and higher devices do not contact the Attack Object Database server URL directly.

- The mode for checking and updating the database (ScreenOS 5.0 devices only):
  
  Notification checks the attack object update server at specified times and notifies you if the database on the server is more recent than the database on the security device.
Update checks the attack object update server at specified times and automatically updates the database on the device if the database on the attack object update server is more recent.

Schedule (daily, weekly, or monthly) on which the security device checks the attack object update server

You can also direct a security device to update its attack object database immediately, either from the attack object update server (ScreenOS 5.0 devices) or the NetScreen-Security Manager GUI Server (ScreenOS 5.1 and higher devices). For details, see Chapter 7, “Managing Devices”.

Disabling Attack Objects

Occasionally, an attack object produces false positives when included in a Security Policy for your network. You can remove the attack from the firewall rule by removing the attack object group to which the attack belongs, or by disabling the individual attack object at the device level. Although disabling attack objects does not improve throughput performance for the security device, this fine-tuning of the attacks detected by each device helps reduce false positives in your logs.

To disable attack objects, the attack object database on the managed device must match the version of the database on the GUI Server. If the databases do not match, the Disable Attacks option does not appear in the device navigation tree, and a validation icon appears next to the Attack Database Version setting in Security > Attack DB > Settings.

To disable an attack object on a device, double-click the device to open the device configuration. In the device navigation tree, select Security > Attack DB > Disable Attacks, then select the attack objects you want to disable.

**NOTE:** Disabled attack objects are device-specific. For example, disabling an attack object within the root system does not disable the attack object in any of its virtual systems, and disabling an attack object in one vsys does not affect that attack object in any other vsys.

For more detailed explanations of the attack object database, see the “Attack Detection and Defense Mechanisms” volume in the NetScreen Concepts & Examples ScreenOS Reference Guide.

Configuring Security Module (SM) Settings

The IDP SM settings specify how the security module(s) on the ISG 2000 or ISG 1000 device handles traffic before it becomes associated with a connection. When you enable and start IDP on the device, default values for all security module parameters are used. As you fine-tune a Security Policy to fit network traffic, you may want to edit these default values. If you make changes to the default settings, the changes only affect that device to which the security module settings apply.

- Configuring Load Time Parameters—Use these options to control how the security module functions when it first powers on.
- Configuring Run-Time Parameters—Use these options to control how the security module operates.
Configuring Protocol Thresholds—Use these options to control how the security module handles packets for specific protocols.

Configuring Load Time Parameters
Use the Load Time Parameters tab to configure the following:

- **Flow table size.** For improved performance, set the flow table size to limit the size of the connection table. This setting should reflect the maximum number of concurrent flows you expect to have at any one time. A TCP connection has about two flows per session, and a UDP connection has about three flows per session. Default setting: The security module connection table can handle 100,000 concurrent flows.

- **Enable or disable log suppression.** Log suppression reduces the number of logs displayed in the Log Viewer by displaying a single record for multiple occurrences of the same event. Log suppression can negatively impact Sensor performance if the reporting interval is set too high. Default setting: Enabled. The security module suppresses multiple instances of the same log record.

- **Include destination IPs while performing log suppression.** When log suppression is enabled, multiple occurrences of events with the same source IP, service, and matching attack object generate a single log record with a count of occurrences. If you enable this option, log suppression only combine logs records for events with a matching source IP as well. Default setting: Not enabled. The security module does not consider destination IP when determining matching events for log suppression.

- **Number of log occurrences after which log suppression begins.** This setting specifies how many instances of a specific event must occur before log suppression begins. When you look at the log records in the Log Viewer, you see this number of log records followed by a combined record for the remaining occurrences within the time interval. Default setting: 1 (log suppression begins with the first occurrence).

- **Maximum number of logs that log suppression can operate on.** When log suppression is enabled, the device must cache log records so that it can identify when multiple occurrences of the same event occur. This setting specifies how many log records are tracked simultaneously by the security device. Default setting: IDP can operate on 16384 log records.

- **Time (seconds) after which suppressed logs will be reported.** When log suppression is enabled, the device maintains a count of multiple occurrences of the same event. After the specified number of seconds has passed, the security device writes a single log entry containing the count of occurrences. Default setting: the device reports suppressed logs after 10 seconds.

Configuring Run-Time Parameters
Use the Run-Time Parameters tab to configure the following:

- **General.** These settings control how the security module handles remote procedure call (RPC) requests and replies and IP fragments. Click the Show button to view and configure these settings.
• Backdoor Detection. These settings control how the security module implements heuristics. These parameters complement the rules in the backdoor rulebase.

• TCP Reassembler. These settings control how the security module handles TCP flows. Click the Show button to view and configure these settings.

For detailed descriptions of each setting, see the NetScreen-Security Manager Online Help.

Configuring Protocol Thresholds
Use the Protocol Thresholds and Configuration tab to control how the security module handles packets for specific types of protocols. Click the Show button to view and configure settings for a specific protocol. For detailed descriptions of each setting, see the NetScreen-Security Manager Online Help.

Configuring Advanced Device Settings

Use the advanced screens to configure advanced options for the security device. In the device navigation tree, select Advanced to view configuration options.

The following sections detail the advanced options for security devices:

• Configuring Timeouts for Predefined Services
• Configuring SIP Settings
• Configuring MGCP Settings
• Configuring H.323 Settings
• Configuring Traffic Shaping
• Configuring Application Layer Gateways (ALGs)
• Configuring Packet Flow
• Configuring Supplemental Command Line Interface (CLI)
• Configuring TFTP/FTP Server Operation
• Configuring Host and Domain Name
• Configuring NSGP
Configuring Timeouts for Predefined Services

Use the Predefined Service Timeout option to configure timeouts for predefined services. Services are types of IP traffic for which protocol standards exist. Each service has a port number associated with it, where the access policy accepts a request for that service. When you create an access policy, you must define a service for it. You can select one of the predefined services or select a custom service that you have created. For predefined services, you can use the default timeout specified by the protocol or you can configure a different timeout value.

To configure a timeout for a predefined service:

1. Click the Add icon in the Predefined Service Timeout configuration screen. The Predefined Service Timeout dialog box appears.
2. Select the service from the Name scrolling list.
3. Select User-defined Value from the Timeout scrolling list.
4. Enter the timeout value.
5. Click OK.

For more detailed explanation about configuring timeouts for predefined services on security devices, see the “Fundamentals” volume in the NetScreen Concepts & Examples ScreenOS Reference Guide.

NOTE: For security devices running ScreenOS 5.2 and higher, you can also configure predefined service timeouts on virtual systems.

Configuring SIP Settings

Use the SIP Settings option to configure Session Initiation Protocol (SIP) as a service on the security device. SIP is an Internet Engineering Task Force (IETF)-standard protocol for initiating, modifying, and terminating multimedia sessions (such as conferencing, telephony, or multimedia) over the Internet. SIP is used to distribute the session description, to negotiate and modify the parameters of an existing session, and to terminate a multimedia session.

The device can then screen SIP traffic, permitting or denying it based on a Security Policy that you configure. SIP is a predefined service in ScreenOS and uses port 5060 as the destination port. Security devices currently do not support NAT (network address translation) with SIP.

SIP is used to distribute the session description and, during the session, to negotiate and modify the parameters of the session. SIP is also used to terminate the session.

SIP messages consist of requests from client to server and responses to requests from servers to clients with the purpose of establishing a session (or a call). A UA (User Agent) is an application that runs at the endpoints of the call and consists of two parts: the UAC (User Agent Client) that sends SIP requests on behalf of the user, and a UAS (User Agent Server) who listens to the responses and notifies the user when they arrive. Examples of User Agents are SIP proxy servers and SIP phones.
A call can have one or more voice channels. Each voice channel has two sessions (or two media streams), one for RTP and one for RTCP. When managing the sessions, the security device considers the sessions in each voice channel as one group. Settings such as the inactivity timeout apply to a group as opposed to each session.

Setting SIP Inactivity Timeouts
You can configure the following types of inactivity timeouts that determine the lifetime of a group:

- **Signaling Inactivity Timeout**—This parameter indicates the maximum length of time (in seconds) a call can remain active without any SIP signaling traffic. Each time a SIP signaling message occurs within a call, this timeout resets. The default setting is 43200 seconds (12 hours).

- **Media Inactivity Timeout**—This parameter indicates the maximum length of time (in seconds) a call can remain active without any media (RTP or RTCP) traffic within a group. Each time a RTP or RTCP packet occurs within a call, this timeout resets. The default setting is 120 seconds.

If either of these timeouts expire, the security device removes all sessions for this call from its table, thus terminating the call.

Select any of the appropriate checkboxes to pass messages that cannot be decoded by the device in either Route Mode or NAT Mode:

- Pass Nonparsable packets in Router Mode
- Pass Nonparsable packets in NAT Mode

Configuring SIP Firewall Features
Multiple SIP INVITE requests can overwhelm a SIP proxy server. You can configure the security device to monitor INVITE requests (and the proxy server replies) to protect SIP proxy servers.

- **SIP Attack Protection**—To drop multiple, identical SIP INVITE messages, configure SIP Attack Protection and enter the number of seconds for which you want to drop similar packets. If SIP proxy server reply contains a 3xx, 4xx, or 5xx response code, the ALG stores the source IP address of the request and the IP address of the proxy server in a table. The security device checks all INVITE requests against this table and discards matching packets for the specified number of seconds.

- **Destination IP Server Protection**—To protect a specific SIP proxy server from multiple identical SIP INVITE requests, configure Destination IP Server Protection for a specific IP address and netmask.

  - If you do not specify a specific SIP proxy server, SIP Attack Protection monitors all SIP traffic for multiple identical SIP INVITE messages.

  - If you do specify a specific SIP proxy server, SIP Attack Protection monitors only SIP traffic destined for the specified SIP proxy server.
For more detailed explanation about configuring SIP on security devices, see the "Fundamentals" volume in the NetScreen Concepts & Examples ScreenOS Reference Guide.

**Configuring MGCP Settings**

Use the MGCP Settings option to configure Media Gateway Control Protocol (MGCP). MGCP is a text-based, application layer protocol that can be used for call setup and call control. The protocol is based on a master/slave call control architecture: the media gateway controller (call agent) maintains call control intelligence, and media gateways carry out the instructions from the call agent.

**Setting MGCP Inactivity Timeouts**

You can configure the following types of inactivity timeouts that determine the lifetime of a group:

- **Inactive Media Timeout in seconds**—This parameter indicates the range a call can remain inactive without any MGCP traffic. Each time an MGCP message occurs within a call, this timeout resets. If the timeout value is reached, the security device removes all sessions for this call from its table, thus terminating the call. The default setting is 120 seconds and the range of values is 10-255 seconds.

- **Transaction Timeout in seconds**—This parameter indicates the range of time a call can remain inactive between the gateway and the Certificate Authority (CA). If the timeout value is reached, the security device removes all sessions for this call from its table, thus terminating the call. The default setting is 30 seconds and the available values range from 5-50 seconds.

- **Maximum call duration in minutes**—This parameter indicates the maximum length of time a call can remain inactive between the gateway and the Certificate Authority (CA). The call is cleared if the transaction times out. The default is 720 minutes.

As a firewall, it might be necessary to parse all messages strictly and drop the unidentified messages. However, the following options are available to pass messages that cannot be decoded by the device in either Route Mode or NAT Mode:

- **Pass unidentified MGCP message in route mode**
- **Pass unidentified MGCP message in nat mode**

**Configuring MGCP Firewall Features**

The MGCP firewall features allow you to enable flood protection to and from the gateway.

- **Connection Flood Protection to/from Gateway**—Control pinhole connections by setting a limit to the rate of CRCX command processing. CRCX commands that exceed the limit are dropped. The range is 1-65,535 and the default is 1,000.

- **Message Flood Protection to/from Gateway**—Messages are dropped if they arrive at a rate (in seconds) higher than the configured rate. The range is 1-200 and the default is 200 seconds.
For more detailed explanation about configuring MGCP on security devices, see the “Fundamentals” volume in the NetScreen Concepts & Examples ScreenOS Reference Guide.

**Configuring H.323 Settings**

H.323 application layer gateway (ALG) lets you to secure Voice-over-IP (VoIP) communication between terminal hosts, such as IP phones and multimedia devices. In such a telephony system, gatekeeper devices manage call registration, admission, and call status for VoIP calls. Gatekeepers can reside in the two different zones, or in the same zone.

The H.323 protocol ALG is enhanced to support incoming calls in NAT mode and slow start in gatekeeper routed mode. In gatekeeper routed mode, all control channel negotiations (Q.931 and H.245) are performed between the gatekeeper and the end points. The media channels, on the other hand, are opened directly between the end points.

**Setting H.323 Inactivity Timeouts**

When you enable H.323, the gateway is registered to the flow and reassembly. In addition, the port is also registered. If you do not enable H.323, none are registered. You can configure the following inactivity timeout that determine the lifetime of a group:

- Set incoming-table timeout value—Sets or resets the default timeout value (in seconds) for the NAT table entry. The default value is 3,600 seconds (60 minutes).

Select any of the appropriate checkboxes to pass messages that cannot be decoded by the device in either Route Mode or NAT Mode:

- Pass Nonparsable packets in Router Mode
- Pass Nonparsable packets in NAT Mode

For more detailed explanation about configuring H.323 on security devices, see the “Fundamentals” volume in the NetScreen Concepts & Examples ScreenOS Reference Guide.

**Configuring Traffic Shaping**

Use the traffic shaping option to allocate an appropriate amount of network bandwidth to every user and application on a specific device interface. The appropriate amount of bandwidth is defined as cost-effective carrying capacity at a guaranteed Quality of Service (QoS). To classify traffic, you create security policies and specify the amount of guaranteed bandwidth and maximum bandwidth, and the priority for each class of traffic. You can also shape traffic at the policy level to allocate bandwidth for particular types of traffic. For information about using traffic shaping within a rule, see “Configuring Traffic Shaping in a Security Policy” on page 541.
Guaranteed bandwidth and maximum bandwidth are not strictly policy based but, with multiple physical interfaces in the egress zone, are based on both policy and total egress physical interface bandwidth available. The physical bandwidth of every interface is allocated to the guaranteed bandwidth parameter for all policies. If there is any bandwidth left over, it is sharable by any other traffic. In other words, each policy gets its guaranteed bandwidth and shares whatever is left over, on a priority basis (up to the limit of its maximum bandwidth specification), with all other policies. Refer to “Configuring Interface Advanced Properties” on page 227 for more information describing how to configure physical settings on the device interface.

Using the traffic shaping option, you can configure the following traffic shaping parameters:

- **Priority Levels**—You can use the Traffic Shaping screen to perform priority queuing on bandwidth that is not allocated to guaranteed bandwidth, or unused guaranteed bandwidth. Queuing allows the security device to buffer traffic in up to eight different priority queues. The security device maps the eight priority levels to the first three bits in the DiffServ field, or to the IP precedence field in the ToS byte in the IP packet header. By default, the highest priority (priority 0) on the security device maps to 111 in the IP precedence field. The lowest priority (priority 7) maps to 000 in the IP precedence field.

- **Traffic Shaping Mode**—Traffic shaping is automatically determined by the device, but you can set it to on or off.

- **Clear DSCP Class Selector**—The class selector controls the number of bits affected in the DiffServ field. By default, the priority levels affect only the first three bits in the eight bit DiffServ field. The remaining bits are untouched, but can be altered by an upstream router, which might change the IP priority preference. When the DSCP class selector is enabled, the class selector zeroes the remaining five bits in the DiffServ field, which prevents upstream routers from altering priority levels.

For a more detailed explanation about configuring traffic shaping on security devices, see the “Fundamentals” volume in the NetScreen Concepts & Examples ScreenOS Reference Guide.

**Configuring Application Layer Gateways (ALGs)**

Application layer gateways manage specific protocols by intercepting traffic as it passes through the security device. After analyzing the traffic, the ALG allocates resources to permit the traffic to pass securely. By default, all ALGs are enabled on a security device. In situations where a security device is receiving an excessive amount of malicious or accidental traffic of a particular type, you might want to disable the associated ALG.

You can enable or disable the following ALG protocols:

- **H323**—the H323 ALG set includes three ALGs that handle specific tasks for H.323 traffic. To disable H.323 on the security device, you must disable all of the following ALGs:
  
  - **H245**—This ALG is a control signaling protocol used to exchange messages between H.323 endpoints.
- **Q931** — This ALG is a layer 3 protocol used for Integrated Services Digital Network (ISDN) call establishment, maintenance, and termination between H.323 endpoints.

- **RAS** — The Registration, Admission, and Status (RAS) ALG is used to register, control admission, change bandwidth, check status, and perform disengage procedures between H.323 endpoints and gatekeepers.

- **MSRPC** — The Microsoft Remote Procedure Call (MS-RPC) ALG enables a program running on one host to call procedures in a program running on another host. Because of the large number of RPC services and the need to broadcast, the transport address of an RPC service is dynamically negotiated based on the service program's Universal Unique Identifier (UUID).

- **RTSP** — The Real Time Streaming Protocol (RTSP) is used to control delivery of one or more synchronized streams of multimedia, such as audio and video.

- **SIP** — The Session Initiation Protocol (SIP) is an Internet Engineering Task Force (IETF)-standard protocol for initiating, modifying, and terminating multimedia sessions (such as conferencing, telephony, or multimedia) over the Internet. SIP is used to distribute the session description, to negotiate and modify the parameters of an existing session, and to terminate a multimedia session.

- **SQL** — The SQL ALG is used to handle SQL, a relational database management system.

- **SUNRPC** — The Sun Remote Procedure Call (SUNRPC) enables a program running on one host to call procedures in a program running on another host. Because of the large number of RPC services and the need to broadcast, the transport address of an RPC service is dynamically negotiated based on the service's program number and version number.

- **MGCP** — The Media Gateway Control Protocol (MGCP) is supported on security devices in Route, Transparent, and Network Address Translation (NAT) modes. MGCP is a text-based Application Layer protocol used for call setup and control. MGCP is based on a master-slave call control architecture. The media gateway controller (call agent) maintains call control intelligence, while the media gateways carry out instructions from the call agent.

### Configuring Packet Flow

Use the packet flow options to configure the security device to regulate packet flow, including:

- ICMP Path MTU Discovery
- Allow DNS Reply Without Matched Request
- Allow MAC Cache for Management Traffic
- Allow Unknown MAC Flooding
- Skip TCP Sequence Number Check
- TCP RST Invalid Session
Check TCP SYN Bit Before Create Session

Check TCP SYN Bit Before Create Session for Tunneled Packets

Use SYN-Cookie for SYN Flood Protection

Enforce TCP Sequence Number Check on TCP RST Packet

Use Hub-and-Spoke Policies for Untrust MIP Traffic

Max Fragmented Packet Size

Flow Initial Session Timeout (Seconds)

TCP MSS

All TCP MSS

GRE In TCP MSS

GRE Out TCP MSS

Ageing

The following sections detail each packet flow option.

ICMP Path MTU Discovery

The ICMP Path MTU Discovery option controls how a security device handles a packet that meets the following conditions: the Don’t Fragment (DF) bit is set in the IP header; the packet is intended for IPSec encapsulation, and the size of the packet after encapsulation exceeds the maximum transfer unit (MTU) of the egress interface, which is 1500 bytes:

- When this option is enabled, the security device sends the source host an ICMP message indicating the packet size is too large (ICMP type 3, code 4 “Fragmentation needed and DF set”).

- When this option is disabled, the security device ignores the DF bit, encapsulates the packet, fragments the packet so that none of the fragmented packets exceeds the MTU of the egress interface, and forwards them through the appropriate VPN tunnel.

By default, this option is disabled.

Allow DNS Reply Without Matched Request

Use the Allow DNS Reply Without Matched Request option to control how a security device handles DNS reply packets that do not have a matching DNS request:

- When this option is enabled, the security device does not verify that a DNS reply packet has a matching request.
When this option is disabled and the security device receives an incoming UDP first-packet that has a destination port of 53, the device checks the DNS message packet header to verify that the query (QR) bit is 0 (0 = query message). If the QR bit is 1 (1 = response message) the device drops the packet, does not create a session, and increments the illegal packet flow counter for receiving interface.

By default, this option is disabled.

**Allow MAC Cache for Management Traffic**

Use the Allow MAC Cache for Management Traffic option to control how the security device handles a source MAC address for administrative traffic:

- When this option is enabled, the security device caches the source MAC address from incoming administrative traffic, then uses that address when replying. You might need to enable this option for managed devices that use source-based routing.
- When disabled, the security device does not cache the source MAC address from incoming administrative traffic.

By default, this option is disabled.

**Allow Unknown MAC Flooding**

Use the Allow Unknown MAC Flooding option to control how a security device handles a packet that has a destination MAC address that is not in the MAC learning table:

- When this option is enabled, the security device permits the packet to cross the firewall.
- When this option is disabled, the security device drops the packet and does not permit it to cross the firewall.

By default, this option is enabled.

**Skip TCP Sequence Number Check**

Use the Skip TCP Sequence Number Check to control how a security device handles TCP packets with an out-of-sequence TCP number:

- When this option is enabled, the security device does not monitor the TCP sequence number in TCP segments during stateful inspection.
- When this option is disabled, the security device detects the window scale specified by both hosts in a session and adjusts a window for an acceptable range of sequence numbers according to their specified parameters. The device monitors the sequence numbers in packets sent between these hosts; if the device detects a sequence number outside this range, it drops the packet.

By default, this option is enabled.
TCP RST Invalid Session
Use the TCP RST Invalid Session to control how the security device handles a TCP reset packet (a TCP packet with the RST flag set):

- When this option is enabled and the security device receives a TCP reset packet, the device marks the session for immediate termination.
- When this option is disabled, the security device marks the session to termination after the normal session timeout interval. Normal session timeout intervals for common protocols:
  - The TCP session timeout is 30 minutes.
  - The UDP session timeout is 1 minute.
  - The HTTP session timeout is 5 minutes.

By default, this option is disabled.

Check TCP SYN Bit Before Create Session
Use the TCP SYN Bit Before Create Session option to control how a security device handles a set SYN bit in the first packet of a session:

- When this option is enabled, the security device checks that the SYN bit is set in the first packet of a session. If the SYN bit is not set, the device drops the packet and does not create the session.
- When this option is disabled, the security device does not enforce SYN checking before creating a session.

By default, security devices running ScreenOS 5.1 and higher have this option enabled. However, in previous versions of ScreenOS, this option was disabled. If you upgraded from a ScreenOS release prior to ScreenOS 5.1 and higher and did not change the default setting for this option, SYN checking remains disabled.

Check TCP SYN Bit Before Create Session for Tunneled Packets
Use the TCP SYN Bit Before Create Session for Tunneled Packets option to control how a security device handles a set SYN bit in the first packet of a VPN session:

- When this option is enabled, the security device checks that the SYN bit is set in the first packet arriving in a VPN tunnel. If the SYN bit is not set, the device drops the packet and does not create the session.
- When this option is disabled, the security device does not enforce SYN checking before creating a session in a VPN tunnel.

By default, this option is enabled.

Use SYN-Cookie for SYN Flood Protection
Use the Use SYN-Cookie for SYN Flood Protection option as an alternative to traditional SYN proxying mechanisms to help reduce CPU and memory usage:
When this option is enabled on the security device, SYN-Cookie becomes the TCP-negotiating proxy for the destination server, and replies to each incoming SYN segment with a SYN/ACK containing an encrypted cookie as its Initial Sequence Number (ISN). The cookie is a MD5 hash of the original source address and port number, destination address and port number, and ISN from the original SYN packet. After sending the cookie, the security device drops the original SYN packet and deletes the calculated cookie from memory.

When this option is disabled, traditional SYN-Proxy becomes the TCP-negotiating proxy for the destination server.

By default, this option is disabled.

NOTE: This option is only available on devices running ScreenOS 5.2 and higher.

Enforce TCP Sequence Number Check on TCP RST Packet

Use the Check TCP Sequence Number Check on TCP RST Packet option to control how a security device handles TCP reset (RST) packets with an out-of-sequence TCP number:

- When this option is enabled, the security device monitors the TCP sequence number in a TCP segment with the RST bit enabled. If the sequence number matches the previous sequence number for a packet in that session or is the next higher number incrementally, the device permits the packet to cross the firewall. If the sequence number does not match either of these expected numbers, the device drops the packet and sends the host a TCP ACK segment with the correct sequence number.

- When this option is disabled, the security device does not monitor the TCP sequence number in TCP segments that have a RST bit enabled.

By default, this option is disabled.

NOTE: The NetScreen-5000 series does not support this option.

Use Hub-and-Spoke Policies for Untrust MIP Traffic

Use this option to control how the security device handles the forwarding of packets arriving in a VPN tunnel to and from a mapped IP (MIP) address:

- When this option is enabled, the security device forwards traffic arriving through a VPN tunnel to a mapped IP (MIP) address on one tunnel interface to the MIP host at the end of another VPN tunnel. The two tunnels form a hub-and-spoke configuration, with the traffic looping back on the same outgoing interface.

- When this option is disabled, the security device does not forward VPN traffic arriving at a MIP to a MIP at the other end of the VPN tunnel.
By default, this option is enabled.

**NOTE:** This option affects traffic forwarding only when the outgoing interface is bound to the Untrust zone.

### Max Fragmented Packet Size

Use the Max Fragmented Packet Size option to control the maximum size of a packet fragment generated by the security device. You can set the number value between 1024 and 1500 bytes inclusive. For example, if a received packet is 1500 bytes and this option is set to 1460 bytes, the device generates two fragment packets: The first is 1460 bytes and the second is 40 bytes. If you reset this option to 1024, the first fragment packet is 1024 bytes and the second is 476 bytes.

By default, this option is set to none.

### Flow Initial Session Timeout (Seconds)

Use the Flow Initial Session Timeout to control the number of seconds the security device keeps an initial TCP session in the session table before dropping it or receiving a FIN or RST packet. You can set the number of seconds from 20 seconds to 300 seconds.

By default, this option is set to 20 seconds.

### TCP MSS

Use the TCP MSS option to control how the security device handles the TCP-MSS value for TCP SYN packets in an IPSec VPN tunnel:

- When this option is set to Packet Size, the security device modifies the MSS value in a TCP packet to avoid fragmentation caused by the IPSec operation. The default MSS for this option is 1400.
- When this option is set to Disable, the security device does not modify the MSS value in a TCP packet.

By default, this option is set to Disabled.

**NOTE:** When you configure a value for the All TCP MSS option, that value overrides the settings defined for this option.

### All TCP MSS

Use the All TCP-MSS to control how security device handles the TCP MSS value for TCP SYN packets in all network traffic:

- When this option is set to Packet Size, the security device modifies the MSS value in a TCP packet to avoid fragmentation by other network components. You can set the TCP MSS range from 0 to 65,535 bytes; the default MSS for this option is set to none.
Additionally, this option overrides the configuration for TCP MSS (described above):

- If the TCP MSS option for IPSec VPN traffic is not set, the security device applies the value specified in this option for TCP packets in an IPSec VPN tunnel.

- If the TCP MSS option for IPSec VPN traffic is set, the security device overrides that value with the value from the All TCP MSS option.

- When this option is set to Disable, the security device does not modify the MSS value of a TCP packet in network traffic.

By default, this option is set to Disable.

GRE In TCP MSS

Use the GRE in TCP MSS option to control how security device handles the TCP MSS value for Generic Routing Encapsulation (GRE) packets destined for an IPSec VPN tunnel.

- When this option is set to Packet Size, the security device modifies the MSS value in a GRE packet to avoid fragmentation caused by the IPSec operation. The TCP MSS range is 64 to 1420 bytes inclusive; the default MSS for this option is 1320.

- When this option is set to Disable, the security device does not modify the MSS value in a GRE packet entering an IPSec VPN tunnel.

By default, this option is set to Disable.

GRE Out TCP MSS

Use the GRE Out TCP MSS option to control how security device handles the TCP MSS value for Generic Routing Encapsulation (GRE) packets leaving an IPSec VPN tunnel.

- When this option is set to Packet Size, the security device modifies the MSS value in a GRE packet to avoid fragmentation caused by the IPSec operation. The TCP MSS range is 64 to 1420 bytes inclusive; the default MSS for this option is 1320.

- When this option is set to Disable, the security device does not modify the MSS value in a GRE packet leaving an IPSec VPN tunnel.

By default, this option is set to Disable.

Ageing

Use the Ageing options to control how the security device uses aggressive ageing to affect session timeout. Aggressive ageing begins when the number of entries in the session table exceeds the high-watermark setting, and ends when the number of sessions falls below the low-watermark setting. When aggressive aging is in effect, the security device ages out sessions—beginning with the oldest sessions first—at the rate you specify.
When the session table is in any other state, the normal session timeout value is applied. Normal session timeout intervals for common protocols:

- The TCP session timeout is 30 minutes.
- The UDP session timeout is 1 minute.
- The HTTP session timeout is 5 minutes.

**Early Ageout Time Before the Session's Normal Ageout**

Use this ageing option to control how the security device uses aggressive ageing to age out a session from its session table. The value range is 2 to 10 units, where each unit is 10 seconds; by default, the early-ageout value is 2, or 20 seconds.

**Percentage of Used Sessions Before Early Aging Begins**

Use this ageing option to control when the security device begins aggressive ageing. The value range is 1 to 100, which indicates percent of the session table capacity. By default, this option is set to 100% (used sessions must account for 100% of the session table capacity before aggressive ageing begins).

**Percentage of Used Sessions Before Early Aging Stops**

Use this ageing option to control when the security device ends aggressive ageing. The value range is 1 to 100, which indicates percent of the session table capacity. By default, this option is set to 100% (used sessions must account for 100% of the session table capacity before aggressive ageing ends).

**Configuring Supplemental Command Line Interface (CLI)**

Use the Supplemental CLI option to configure features on security devices not yet formally supported in NetScreen-Security Manager. This applies to security devices running a future release of ScreenOS.

**NOTE:** Supplemental CLI is supported for ScreenOS 5.1 and higher.

**Configuring TFTP/FTP Server Operation**

**NOTE:** It is recommended that you use the Supplemental CLI to configure features in future versions of ScreenOS only. When you perform an update, the CLI commands that you specify are sent unconditionally to the security device. NetScreen-Security Manager does not validate whether or not these commands are sent successfully. Validation errors may occur if you edit the actual configuration on the device using the supplemental CLI.

Use the TFTP/FTP option to configure a security device running to enable TFTP or FTP servers to save or import external files, such as configuration files (.cfg), ScreenOS firmware versions, public keys, error messages, certificates, and other items.
For security devices running ScreenOS 4.0.x or 5.0, NetScreen-Security Manager does not use the TFTP server on the security device to download ScreenOS firmware versions, certificates, and CRLs to the managed device. To perform these tasks, you must install a TFTP server on the NetScreen-Security Manager Device Server. For details, see the NetScreen-Security Manager Installer’s Guide.

NOTE: For security devices running ScreenOS 5.1 and higher, NetScreen-Security Manager uses SSP to download ScreenOS firmware versions, certificates, and CRLs to the managed device.

For TFTP servers, you can specify the following:

- **Source interface**
- **Number of times that the server can retry a TFTP communication before the security device ends the attempt**
- **Timeout (in seconds) before the device terminates an inactive TFTP connection.**

You can also enable FTP servers to dynamically negotiate a data port other than port 20.

For more detailed explanation about configuring TFTP or FTP servers for security devices, see the `ip` commands in the NetScreen CLI Reference Guide.

### Configuring Host and Domain Name

The Host/Domain Name option enables you to configure a host and domain name for the security device. The host name is a character string that identifies the device. The host name, combined with a domain name, enables other devices to access the security device through a DNS server. If you define a fully-qualified domain name (FQDN) for the device, you can use the FQDN as a gateway for a VPN tunnel.

For more detailed explanation about configuring the hostname or domain name for security devices, see the `hostname` and `domain` commands in the NetScreen CLI Reference Guide.

### Configuring NSGP

NetScreen Gatekeeper Protocol (NSGP) is a Juniper Networks proprietary peer-to-peer protocol that enables a security device to act as a server for Voice-over-IP (VoIP) traffic:

- **NetScreen-500 security devices running ScreenOS 5.0GPRS can be both the NSGP server and client.**
- **NetScreen-500 and NetScreen-5000 series security devices running ScreenOS 5.0NSGP or 5.1 and higher can only be an NSGP server.**

NOTE: To use NSGP on a NetScreen-500 or -5000 device, you must first enable NSGP using a license key. For details on activating NSGP using a license key, see “Managing License Keys” on page 418.
You can use NSGP to prevent overbilling attacks that can occur when using GTP for VoIP. By configuring one security device as a NSGP server and another security device as a GTP client, you can keep both server and client aware of the connection status. When a user initiates a call, the NSGP server and GTP client establish a session; when the user completes the call, the client notifies the server, prompting the server to close the session.

Configuring NSGP on a device does not automatically enable the device to handle GTP traffic—it simply enables the GTP client and NSGP server to close a session at the same time. To enable the GTP client to manage GPRS traffic, you must create a GTP object, then add that object to the Security Policy installed on the device. For details on creating a GTP object, see “Configuring GTP Objects” on page 490. For details on adding a GTP Object to a Security Policy, see “Enabling GTP for Firewall Rules” on page 547.

About Overbilling

Because mobile stations get their IP addresses from an IP pool, an overbilling attack can occur when a legitimate subscriber returns an IP address to the IP pool, but the session is still open. Attackers can hijack the IP address without being detected and reported, then download data at the expense of the legitimate subscriber, or send data to other subscribers. Overbilling can also occur when a newly-returned IP address is reassigned to another MS; traffic initiated by the previous MS might be forwarded to the new MS, causing the new MS to be billed for unsolicited traffic. To protect subscribers of a PLMN from Overbilling attacks, you can use the NetScreen Gatekeeper Protocol (NSGP) module and two security devices.

The NSGP module includes two components: the client and the server. The client connects to the server and sends requests, which the server processes. Both client and server support multiple connections to each other and to others simultaneously. Using TCP, NSGP monitors the connectivity between client and server by sending Hello messages at set intervals.

NSGP uses a session context to ensure that the server and client know that status of the connection. The session context stores is identified by a unique number (context ID); when configuring NSGP on the client and server devices, you must use the same context ID on each devices. When the client sends a “clear session” request to the server, the request includes the context ID and IP address of the server. When the server receives the “clear session” message, it matches the context ID and then clears the session from its table.

The security device acting as the NSGP server must run the ScreenOS 5.0GPRS firmware, and the other device acting as the GTP client must run the ScreenOS 5.0NSGP firmware. After you have deployed the two devices, you must:

- Configure NSGP on the GTP server to recognize when a GTP tunnel is deleted and to notify the GTP client.

- Configure NSGP on the GTP client to automatically clear sessions whenever the NSGP server gets a notification from the GTP client that a GTP tunnel was deleted.

By clearing the sessions, the NSGP server stops the unsolicited traffic, and prevents overbilling.
EXAMPLE: CONFIGURING NSGP

In this example, you configure NSGP on both the GTP firewall (client) and the Gi firewall (server). First, you must create the GTP Object for the client connection. Then, to enable NSGP on the security device, you must configure both the server and client side connection parameters:

- For the NSGP server connection, you enable NSGP on an interface.
- For the GTP client connection, you select a source interface, then copy the NSGP server settings (from the NSGP server device) to configure the destination interface.

Finally, you create a firewall rule that includes the GTP object, the GTP firewall, and the Gi firewall.

Figure 85: NSGP Example Overview

1. Create a GTP object named GPRS1. For details and an example for creating a GTP object, see “Configuring GTP Objects” on page 490.

2. Add the Gi Firewall (server) as a NetScreen-500 running 5.1, then configure the network module:
   a. Double-click the device icon to open the device configuration. In the device navigation tree, select Network > Slot.
   b. Double-click slot 1 to display the slot configuration dialog box. For Card Type, select 2 Interfaces (10/100), then click OK.

3. Add the GTP firewall (client) as a NetScreen-500 running 5.0GPRS, then configure the network module:
   a. Double-click the device icon to open the device configuration. In the device navigation tree, select Network > Slot.
   b. Double-click slot 1 to display the slot configuration dialog box. For Card Type, select 2 Interfaces (10/100).
c. Click OK to save the slot configuration.

4. Configure the Gi firewall (server):
   a. In the device navigation tree, select Advanced > NSGP Server Side.
   b. Leave the default port number and enter an MD5 password.
   c. In the NSGP Context IDs area, click the Add icon to display the New Context Entry dialog box. Configure the following, then click OK:
      - For Context Entry, enter 2.
      - For Zone, select untrust.
   d. In the Interface NSGP Settings area, right-click the ethernet 1/2 interface and select Edit. The General Properties screen appears. Configure the following:
      - Ensure that the Zone is untrust and the Mode is Route.
      - For IP Address, enter 2.2.1.4.
      - For Netmask, enter 24.
      - Ensure that Manageable is enabled and that the Management IP is 2.2.1.4.
   e. In the interface navigation tree, select Service Options. Configure the following:
      - Select Telnet.
      - Select NSGP Enabled.
      - Select Enforce IPSec to encrypt the GTP connection.
   f. Click OK to save your changes to the interface, then click OK to save your changes to the device.

5. Configure the GTP firewall (client):
   a. In the device navigation tree, select Advanced > NSGP > NSGP Connections. Click the Add icon to display the New NSGP Connection dialog box.
   b. For Source Interface, select ethernet 1/2.
   c. For Destination, click Copy Existing NSGP Server Setting. The Copy Existing NSGP Server Info dialog box appears. Configure the following:
      - For NSGP Server Info, select Gi firewall (server).
      - For Destination Interface, select ethernet 1/2.
d. Click OK to copy the NSGP server settings to the GTP client. NetScreen-Security Manager automatically completes the destination server settings for the GTP client.

e. In GTP Objects, select the GPRS1 object. When complete, your NSGP connection settings for the GTP client should appear as shown below:

Figure 86: NSGP Connection Dialog Box

f. Click OK to save the NSGP Connection.

6. Configure a firewall rule to handle GTP traffic, as shown below:

Figure 87: Configure Firewall Rule for GTP Traffic
Configuring L2TP and XAuth Local Users

Use the L2TP/XAuth/Local User option to enable the security device to authenticate local users and/or assign specific IP pools and remote settings. Because user objects are shared objects, you can configure the same user on multiple devices, but assign different remote settings and IP pool for each device.

You must configure a L2TP or XAuth local user on a security device when:

- You want the device to authenticate the user. Typically, you want to authenticate a user who is connecting to the device using a VPN tunnel.
- You want the device to assign specific IP, DNS server, and WINS server addresses to a user who is connecting to the device using a VPN tunnel. The remote settings and IP pool you assign at the device level override the remote settings and IP pool assigned to the VPN.

Configuring L2TP Local Users

The Layer 2 Tunneling Protocol (L2TP) enables a security device to authenticate users using the local database or an external auth server, and assign specific remote settings and IP pools.

L2TP simply enables the security device to authenticate users; to encrypt an L2TP VPN tunnel, you must apply an encryption scheme, such as IPSec, to the L2TP tunnel. When configuring an L2TP-over-IPSec VPN, you are actually setting up an L2TP tunnel and an IPSec tunnel with the same endpoints, then linking the two tunnels together in a Security Policy rule. VPN Manager automatically generates the required rules; if you are creating the L2TP-over-IPSec VPN at the device-level, you must configure the rules manually. For more details on L2TP VPNs, see “Creating L2TP VPNs” on page 666.

You can also use the device to assign specific IP, DNS server, and WINS server addresses from the local database or a RADIUS server. When you assign the L2TP user or user group a remote setting and IP pool at the device level, the settings override the remote settings and IP pool assigned to the VPN. You can even use different auth servers, one for each aspect of L2TP. For example, you might use a SecurID server to authenticate an L2TP user but make the address assignments from the local database.

Figure 88: Configure L2TP Local User

L2TP User Authentication

Local Database

SecurID

RADIUS

LDAP

L2TP User IP, DNS Server, and WINS Server Address Assignments

Local Database

SecurID

RADIUS

LDAP

X
EXAMPLE: CONFIGURING AN L2TP LOCAL USER

1. In the main navigation tree, select Object Manager > User Objects > Local Users. In the main display area, click the Add icon. Configure the following settings, then click OK:
   - For Name, enter Adam.
   - For Color, select orange.
   - Select Enable, then select L2TP.
   - Select Password, then enter and confirm the password: AJbioJ15.

For details on creating user objects, see “Configuring User Objects” on page 511.

2. In the main navigation tree, select Object Manager > Remote Settings. In the main display area, click the Add icon. Configure the following settings, then click OK:
   - For Name, enter RM_L2TP
   - For Color, select green.
   - Enter Comments, if desired.
   - For Dns1, enter 1.1.1.2.
   - For Dns2, enter 1.1.1.3.
   - For Wins1, enter 0.0.0.0.
   - For Wins2, enter 0.0.0.0.

For details on creating Remote Settings objects, see “Configuring Remote Settings” on page 519.

3. In the main navigation tree, select Object Manager > IP Pools. Configure the new IP Pool:
   a. In the main display area, click the Add icon. The New IP Pool dialog box appears. Configure the following settings:
      - For IP Pool Name, enter Global.
      - For Color, select magenta.
      - Enter Comments, if desired.
   b. Click the Add icon. Configure the following settings and click OK:
      - For Start IP, enter 10.10.2.100.
      - For End IP, enter 10.10.2.180.
c. Click OK to save the new IP Pool object. For details on creating IP Pool objects, see “Configuring IP Pools” on page 515.

4. Configure the L2TP local user:

a. In the main navigation tree, select Device Manager > Security Devices, then double-click the device on which you want to configure the L2TP local user. The device configuration appears.

b. In the device navigation tree, select L2TP/XAuth/Local User, then click the Add icon. The new L2TP/XAuth User Settings dialog box appears. Configure the following settings, then click OK:
   - For User, select Adam.
   - For Remote Settings, select RM_L2TP.
   - For IP Pool, select Global.

5. Click OK to save your changes to the device configuration.

About XAuth Users

The XAuth protocol enables the device to authenticate XAuth users and/or assign IP pools and remote settings.

An XAuth user (or user group) is a RAS user who authenticates when connecting to the security device using an AutoKey IKE VPN tunnel. Although both IKE and XAuth users can authenticate through an AutoKey IKE VPN tunnel, the authentication of IKE users is actually the authentication of VPN gateways or clients, while the authentication of XAuth users is the authentication of the individuals themselves. XAuth users must enter information that only they are supposed to know—their user name and password.

You can also assign an XAuth user IP, WINS, and DNS addresses from the device. When you assign the XAuth user or user group a remote setting and IP pool at the device level, the settings override the remote settings and IP pool assigned to the VPN.

For more details about configuring authentication users on security devices, see the “Fundamentals” volume in the NetScreen Concepts & Examples ScreenOS Reference Guide.

Configuring vsys

A vsys is a virtual system that exists within a physical security device. By logically partitioning a single, physical security device into multiple virtual systems (each in its own domain), you can provide secure multi-tenant services. The physical device (known as the “root” device) shares some settings across all vsys, but each vsys also has its own unique settings. To enable the physical device to correctly route traffic to the appropriate vsys device, you must use VLAN tags at the vsys level or IP classification at the root level.
To add a vsys to the NetScreen-Security Manager system, you must first add a physical device that can contain vsys devices (Netscreen-500, 5000 series, ISG 1000, and ISG 2000 security devices support vsys), then add each vsys to the physical device. A NetScreen-Security Manager administrator with full device configuration permissions can see both the root and vsys devices in a domain, but an administrator with only vsys permissions can see only the vsys devices in a domain. To create a secure, multi-tenant system, place the root device in the global domain and each vsys device in its own domain, then assign Vsys administrations to manage each domain. For details on adding a vsys, see “Adding Vsys Devices” on page 111.

After you have added or modeled a new root device and vsys to the NetScreen-Security Manager system, you must configure the vsys interfaces and subinterfaces, and any shared virtual routers and shared security zones on the root device. When importing an existing root device and vsys, NetScreen-Security Manager automatically imports the existing root and vsys settings from each device (physical and virtual).

The NetScreen-5000 series security devices running ScreenOS 5.0 L2V also support vsys transparent mode, also known as layer 2 vsys, or L2V vsys. To create an L2V vsys, when modeling the root device into NetScreen-Security Manager, ensure that the mode is set to Transparent (for imported devices, you must enable transparent mode on the physical device using the WebUI or CLI).

For more details on configuring vsys, refer to the “Virtual Systems” volume in the NetScreen Concepts & Examples ScreenOS Reference Guide. For more details on configuring transparent vsys, refer to the Juniper Networks New Features Guide for ScreenOS 5.0-L2V software.

### Viewing Root and Vsys Configurations

To view a root system configuration, in the main navigation tree, select Device Manager > Security Devices, then double-click the root device. To view the vsys devices associated with the root system, in the device navigation tree, select VSYS.

To view a vsys configuration, in the main navigation tree, select Device Manager > Security Devices, then double-click the vsys. A virtual system configuration is similar to a device configuration, but a vsys configuration displays fewer settings because the root device controls some settings.

### Configuring Virtual Routers for Root and Vsys

At the root level, you can configure a virtual router as shareable, enabling that VR to be used by all vsys. By default, the untrust-vr is shared. To unshare a VR, you must remove all assigned vsys from a shared VR.

At the vsys level, you can configure the following virtual routers:

- Shared root-level virtual routers—By default, the root and vsys share the untrust-vr. However, you can configure a vsys to use any VR that is shared at the root-level.
Non-sharable vsys-level virtual router—This is a vsys-specific virtual router that, by default, maintains the routing table for the Trust-vsysname zone. By default, a vsys-level virtual router is named vsysname-vr (you can also customize the name to make it more meaningful). All vsys-level virtual routers are non-sharable.

Configuring Zones for Root and Vsxs

At the root-level, you can configure a zone as shareable, enabling that zone to be used by all vsxs. To share a zone, the zone must be in a shared virtual router; however, a shared virtual router can contain both shared and unshared zones.

At the vsxs level, the following zones are automatically created or inherited:

- All shared zones—These zones are inherited from the root device.
- Shared Null zone—This zone is inherited from the root device.
- Trust-vsys_name zone—This zone is created by default when you create the vsxs.
- Untrust-Tun-vsys_name zone—This zone is created by default when you create the vsxs.
- Global-vsys_name zone—This zone is created by default when you create the vsxs.

Each vsxs also supports user-defined security zones; you can bind these zones to any shared virtual routers defined at the root level or to the virtual router dedicated to that vsxs.

Configuring Interfaces for Root and Vsxs

Interfaces can be dedicated, shared, imported, and exported between root and vsxs.

At the root level, shared interfaces that are bound to a shared zone. However, any physical, subinterface, redundant interface, or aggregate interface in the root system that is bound to a non-sharable zone is dedicated to the root system, and cannot be shared. To import an interface to a vsxs, the interface must be in the Null zone at the root level; to export an interface from a vsxs, the interface must be in the Null zone at the vsxs level.

At the vsxs level, you can configure the following interfaces:
- **Shared Interface**—A shared interface is an interface that can be shared with the root system. To share a root interface, the interface must be shared at the root level and bound to a shared zone in a shared virtual router. By default, the untrust-vr and Untrust zone are shared, enabling you to configure a vsys to share any root-level physical interface, subinterface, redundant interface, or aggregate interface that is bound to the Untrust zone.

- **Dedicated Subinterface**—A dedicated subinterface uses VLAN tagging, which enables the device to determine the vsys to which inbound or outbound traffic through that interface belongs. When you configure a subinterface in a vsys, the interface is dedicated to that vsys.

- **Imported Physical/Aggregate**—A physical or aggregate interface in the null zone is imported from the root system, then bound to a shared zone or the Trust-vsys vsys zone. When you import a physical or aggregate interface from the root system, the vsys has exclusive use of that interface. You can also export interfaces in the null zone to the root system. When you export a interface to the root system, the root system has exclusive use of that interface.

**Using the VLAN Management Interface**

To manage a vsys independent of the root system, you can create a management interface bound to the VLAN zone (automatically created when you create a vsys). Using the VLAN management interface, a vsys admin can manage the vsys using a unique IP address and VLAN ID.

You can bind more than one interface to the management zone.

**Routing Traffic to Vsys**

To enable the physical device to correctly route traffic to the appropriate vsys device, you must use VLAN IDs (VIDs) at the vsys level or IP classification at the root level.

**Using VLAN IDs**

When using VIDs for routing traffic to vsys, you create dedicated vsys subinterfaces with a VID; all traffic handled by a subinterface includes the subinterface's VID in the frame header. The root system uses the VID to correctly route traffic to and from the subinterface.

---

**NOTE:** A VLAN identifier is also known as a VLAN tag.

A subinterface stems from a physical interface, which acts as a trunk port. A trunk port enables a Layer 2 network device to bundle traffic from several VLANs through a single physical port, sorting the various packets by the VID in their frame headers. VLAN trunking enables one physical interface to support multiple logical subinterfaces, each of which must be identified by a unique VID. The VID on an incoming ethernet frame indicates the destination subinterface—and system. When you associate a VLAN with an interface or subinterface, the device automatically defines the physical port as a trunk port.
Using VLANS in Transparent Mode

When the root device is in Transparent mode, you cannot use VLAN tagging at the vsys level (except when using L2V; for details, see “Configuring Layer 2 Vsys (L2V)” on page 362). However, you can configure subinterfaces and VLAN tagging at the root level by define all physical ports as trunk ports. To do so, in the device navigation tree, select Network > Interfaces, then doubleclick the VLAN-1 interface. In the General Properties interface screen, select Vlan Trunk.

NOTE: The NetScreen-5000 series security devices running ScreenOS 5.0 L2V supports vsys transparent mode, also known as layer 2 vsys, or L2V vsys.

EXAMPLE: USING VLAN TAGS AT VSYS LEVEL

In this example, you define 3 subinterfaces (10.1.1.1/24, 10.2.2.1/24, and 1.3.3.1/24) with VLAN tags on ethernet 2.3 for the three virtual systems vsys1, vsys2, and vsys3. The first two subinterfaces are for two private virtual systems operating in NAT mode, and the third subinterface is for a public virtual system operating in Route mode. All virtual systems share the Untrust zone and its interface with the root system. The Untrust zone is in the untrust-vr routing domain. For vsys1 and vsys2, you use the default virtual router. For vsys3, you choose the sharable root-level untrust-vr.

1. Add a NetScreen-5000 security device in running ScreenOS 5.2 as the root system, then configure the network module:
   a. Double-click the device to open the device configuration. In the device navigation tree, select Network > Slot.
   b. Double-click slot 2 to display the slot configuration dialog box. For Card Type, select 5000-8G SPM.
   c. Click OK to save the slot configuration.

2. Add three vsys devices:
   - Vsys1 and Vsys 2 use the default virtual router
   - Vsys3 uses the existing untrust-vr virtual router

3. Create subinterface for vsys1
   a. In the main navigation tree, select Device Manager > Security Devices, then doubleclick vsys1.
   b. In the device navigation tree, select Network > Interfaces. Click the Add icon and select Sub Interface.
   c. In the subinterface general properties, configure the following then click OK:
      - For Interface, select ethernet2/3.1
      - For Sub Interface Type, select tag.
4. Create subinterface for vsys2
   a. In the main navigation tree, select Device Manager > Security Devices, then double-click vsys2.
   b. In the device navigation tree, select Network > Interfaces. Click the Add icon and select Sub Interface.
   c. In the subinterface general properties, configure the following then click OK:
      - For Interface, select ethernet2/3.2
      - For Sub Interface Type, select tag.
      - For VLAN tag, select 2.
      - For Zone, select trust-vsys2
      - For IP Address and Netmask, enter 10.2.2.1/24

5. Create subinterface for vsys3
   a. In the main navigation tree, select Device Manager > Security Devices, then double-click vsys3.
   b. In the device navigation tree, select Network > Interfaces. Click the Add icon and select Sub Interface.
   c. In the subinterface general properties, configure the following then click OK:
      - For Interface, select ethernet2/3.3
      - For Sub Interface Type, select tag.
      - For VLAN tag, select 3.
      - For Zone, select trust-vsys3
      - For IP Address and Netmask, enter 1.3.3.1/24
      - For Mode, select Route.
Using IP Classification

When using IP-based classification, you associate a subnet or range of IP addresses with the root or a specific vsys. The root system checks the source and destination IP addresses in IP packet headers to identify the device (root or vsys) to which traffic belongs.

You configure IP classification at the root level, on the Untrust interface, which is shared by default with all vsys. In the device navigation tree of the root system, select Network > Interfaces, then double-click the Untrust interface. In the interface navigation tree, select IP Classification, then select Enabled. Right-click and select New to display the New IP Classification List, then configure a subnet or IP address range for the root and/or each vsys.

EXAMPLE: USING IP CLASSIFICATION

In this example, you configure IP-based traffic classification for three virtual systems (vsys1, vsys3, and vsys3). You define the trust-vr as sharable, then create a new, shared zone called internal that is bound to the trust-vr (both internal and Untrust zones are in the shared trust-vr routing domain). Within the internal zone, configure a subnet for each vsys (10.1.1.0/24 for vsys1, 10.1.2.0/24 for vsys2, and 10.1.3.0/24 for vsys3).

Next, bind the interfaces. Configure ethernet1/1 in the shared internal zone, assign IP address 10.1.0.1/16, and select NAT mode. Configure ethernet1/2 in the shared Untrust zone and assign it IP address 210.1.1.1/24. Finally, configure the default gateway in the Untrust zone as 210.1.1.250.

1. Add an ISG 2000 security device running ScreenOS 5.2 as the root system, then configure the network module:
   a. Double-click the device to open the device configuration. In the device navigation tree, select Network > Slot.
   b. Double-click Slot 1 to display the slot configuration dialog box. For Card Type, select 8 Interfaces (10/100).
   c. Click OK to save the slot configuration.

2. Add the following vsys devices (all use default virtual router)
   - vsys1
   - vsys2
   - vsys3

3. In the device navigation tree, select Network > Virtual Routers, then double-click the trust-vr. Ensure that Shared Virtual Router is selected, then click OK.

4. In the device navigation tree, select Network > Zones. Click the Add icon and select New Security Zone. In the Zone General Properties, configure the following:
   - For Name, enter internal
For Virtual Router, select trust-vr

Select Shared. When selected, the option IP Classification appears in the zone navigation tree.

5. In the zone navigation tree, select IP Classification, then configure the following:
   a. Select Enabled.
   b. Right click in the IP Classification screen and select New. The New IP Classification list appears. Configure the following, then click OK:
      - For Vsys, select vsys1
      - Select Subnet
      - For IP Address and Netmask, enter 10.1.1.0/24
   c. Right click in the IP Classification screen and select New. The New IP Classification list appears. Configure the following, then click OK:
      - For Vsys, select vsys2
      - Select Subnet
      - For IP Address and Netmask, enter 10.1.2.0/24
   d. Right click in the IP Classification screen and select New. The New IP Classification list appears. Configure the following, then click OK:
      - For Vsys, select vsys3
      - Select Subnet
      - For IP Address and Netmask, enter 10.1.3.0/24

6. In the device navigation tree, select Network > Interfaces:
   a. Doubleclick ethernet 1/1. In the Interface General Properties, configure the following, then click OK:
      - For Zone, select internal.
      - For IP Address and Netmask, enter 10.1.0.1/16
   b. Doubleclick ethernet 1/2. In the Interface General Properties, configure the following, then click OK:
      - For Zone, select Untrust.
      - For IP Address and Netmask, enter 210.1.1.1/24

7. In the device navigation tree, select Network > Virtual Routers, then doubleclick the trust-vr.
Configuring vsys

a. In the virtual router navigation tree, select Routing Table.

b. In the Destination-based Routing Table area, click the Add icon. Configure the following route, then click OK:

- For IP Address and Netmask, enter 0.0.0.0/0.
- For Next Hope, select Gateway.
- For Interface, select ethernet1/2
- For Gateway IP Address, enter 210.1.1.250

Configuring Layer 2 Vsys (L2V)

A NetScreen-5000 series security device running ScreenOS 5.0-L2V supports virtual systems in transparent mode (the device functions similar to a Layer-2 switch or bridge). The device groups packets to or from a unique vsys based on the VLAN tag in the packet header, applies the Security Policy for the vsys to the packets, then sends permitted packets through the device without packet modification.

When you first add a NetScreen-5000 series security device running ScreenOS 5.0-L2V to NetScreen-Security Manager, the device is in neutral mode, meaning that neither L2V or VLAN trunk mode is configured on the device. To confirm that the device is neutral mode, ensure that the root system does not contain a VLAN group, no VLAN IDS have been exported to a vsys device, vlan1 exists in the root system only, and that the VLAN trunk mode is disabled.

To enable L2V on a neutral root system, you must:

1. Import VLAN IDs from the root system to vsys.
2. Create a VLAN group (in the root system or vsys) and assign that group to a physical port and zone.

Assigning L2V VLAN IDs

You must use VLAN tags for vsys devices in transparent mode. The device classifies traffic to or from the vsys based on the VLAN tag. A root device running ScreenOS 5.0-L2V supports a maximum of 4094 VLANs. You can assign each vsys 2 to 4094 VLANs, however, after a VLAN is assigned to one vsys it cannot be used in another. The root system reserves vlan 1, vlan0, and vlan4095.

By default, all VLAN IDS belong to the root system. To configure VLAN IDs for each vsys, you must import the VLAN IDs from the root system to a vsys:

1. In the main navigation tree, select Device Manager > Security Devices, then doubleclick a vsys device.
2. In the vsys device navigation tree, select Network > Vlan > Import.

NOTE: When L2V is enabled, you cannot configure VLAN trunk mode (option is disabled). For details on changing an L2V root system to VLAN trunk mode, see “Converting L2V to VLAN Trunking” on page 365.
3. Click the Add icon to display the New Vlan Import Entry dialog box, then enter the range of VLAN IDs you want to import from the root system to the vsys.

4. Click OK. NetScreen-Security Manager imports the VLAN IDs within the specified range from the root system; these IDs are now reserved and cannot be used by the root system or other vsys.

To export VLAN IDs to the root system, you must delete the VLAN IDs from the vsys (select the VLAN import entry then click the Delete icon). When you delete an ID range, NetScreen-Security Manager no longer reserves those IDs, enabling you to import the IDs to another vsys.

After you have imported VLAN IDs to a vsys, you can group those IDs and assign them to a physical port and zone.

Creating L2V VLAN Groups
A VLAN group contains VLAN IDs and specifies the port and zone on the physical device that handles those IDs. You can create a VLAN group that includes a single ID range, or add multiple ID ranges to group multiple VLAN ranges.

For each group, you must configure:

- The VLAN IDS ranges you want to include in the group. To include a ID range within a group, you must have previously imported the IDs to the vsys (the IDs must be reserved by the vsys). To view the VLAN IDs imported to the vsys, select the option Show Vlan IDs Imported (option is located at the bottom of the VLAN Group screen). To clear the VLAN ID information from the group screen, clear (unselect) the option.

- The Port and Zone that handle traffic with the specified IDs. You can select any physical interface or aggregate interface and any L2 zone. Interfaces included within an aggregate interface are not displayed and cannot be selected.

  If you select the Null zone for a VLAN interface, NetScreen-Security Manager automatically sets the zone as v1-null.

You can create VLAN groups at the root level and at the vsys level. When configuring a root VLAN group, however, any VLAN ID ranges you include in the group are automatically reserved for the root system and cannot be imported by a vsys.

You cannot delete VLAN IDs that are included in a VLAN group.

Configuring L2V Zones
You can configure any pre-defined zone in a shared virtual router as shareable. In the NetScreen-Security Manager UI, the following pre-defined L2 zones appear with regular zone names:

- v1-trust appears as trust
- v1-untrust appears as untrust
- v1-dmz appears as dmz
The exception is v1-null, which appears as v1-null; the regular null zone is unchanged, and appears as null. By default, the pre-defined VLAN zone is also sharable when using L2V. The VLAN zone contains all vsys management interfaces.

You can also create custom L2V zones in the root system or vsys, although you cannot configure a custom L2V zone as sharable. When you define a new L2 zone, NetScreen-Security Manager prepends the prefix “L2-” to the name during a device update. However, the L2 prefix does not appear in the NetScreen-Security Manager UI. For example, if you create an L2 zone named “music”, the UI displays the zone name as “music”, but the WebUI and CLI displays the zone name as “L2-music”.

NOTE: When configuring a custom L2V zone, the name must include only lower-case letters.

Configuring L2V Interfaces
In the root system, you can bind any interface to an L2 zone. If the zone is shared with vsys, the interface also becomes shared with vsys. You cannot import or export interfaces between root and vsys, and you cannot assign an IP address to an interface (except the VLAN management interfaces).

In the root system, you can create VLAN management interfaces and aggregate interfaces. At the vsys level, you can only create VLAN management interfaces.

Configuring L2V VLAN Management Interfaces
The root system contains a pre-defined VLAN management interface (vlan1) that is bound to the VLAN zone. You can configure this interface as you would a normal security interface, for example, assign the interface an IP address, configure DHCP, or configure monitoring.

For each vsys that you want to manage, you must create the VLAN management interface on the vsys, then bind the interface to the VLAN zone. Because each VLAN interface uses a VLAN ID, you must have previously imported VLAN IDs from a root system before creating the VLAN interface on a vsys device. For example, before you create vlan.3 management interface on a vsys, you must import the VLAN ID 3 from the root system.

For both root and vsys, the VLAN interface name is the VLAN ID for the interface. To add multiple management interfaces, bind each interface to the VLAN zone and assign each interface a unique vlan name (vlan1, vlan2, vlan3, and so on; acceptable range is 2-4094). When assigning IP address to each interface, ensure that the IP subnets for all interfaces do not overlap.

Configuring L2V Aggregate Interfaces
You can create aggregate interfaces in the root system to increase available bandwidth. An aggregate interface must be bound to an L2 zone (cannot be bound to the VLAN zone) and can be shared with vsys. Although you can manage this interface, you cannot assign an IP address. Additionally, if you bind a regular interface to an L2 aggregate interface, you cannot select the zone for the regular interface.

You cannot create aggregate interfaces at the vsys level.
The 8G Secure Port Module (SPM) supports two ASICs; ports ethernet2/1 through ethernet2/4 use one ASIC, and ports ethernet2/5 through ethernet2/8 use the other. You must configure aggregate interfaces in pairs, starting with port ethernet2/1, as shown below:

Figure 89: 8G SPM Aggregate Interfaces

| aggregate1 | ethernet2/1 and ethernet2/2 |
| aggregate2 | ethernet2/3 and ethernet2/4 |
| aggregate3 | ethernet2/5 and ethernet2/6 |
| aggregate4 | ethernet2/7 and ethernet2/8 |

The 8G2 Secure Port Module (SPM) supports a maximum of two 4-port aggregate interfaces, four trusted and four untrusted. Assigning the VLANs to an aggregate interface provides a traffic bandwidth of 2Gps in each direction, with a maximum of 4Gps for bi-directional traffic per Application-Specific Integrated Circuit (ASIC). You must configure aggregate interfaces in pairs, starting with port ethernet2/1, as shown below:

Figure 90: 8G2 SPM and the 5000M2 Management Module

| aggregate1 | ethernet2/1, ethernet2/2, ethernet2/3, and ethernet2/4 |
| aggregate2 | ethernet2/5, ethernet2/6, ethernet2/7, and ethernet2/8 |

Converting L2V to VLAN Trunking

When the VLAN interface is set to Trunk mode, the root system operates in VLAN trunk mode and L2V is disabled for the device. While in VLAN trunk mode, all L2V functionality is unsupported: You cannot import VLAN IDs to vsys devices or VLAN groups to root or vsys.

To change a neutral root system to VLAN Trunk mode, in the device navigation tree, select Network > Interfaces, then doubleclick the vlan1 interface. In the General Properties interface screen, select Vlan Trunk. To disable VLAN trunk mode, clear the Vlan Trunk option (the device returns to neutral).

To change an L2V root device to VLAN Trunk mode, you must first delete VLAN IDs that were imported to vsys devices and VLAN groups in the root and vsys devices.

NOTE: To confirm that the device is neutral mode, ensure that the root system does not contain a VLAN group, no VLAN IDS have been exported to a vsys device, vlan1 exists in the root system only, and that the VLAN trunk mode is disabled.

EXAMPLE: CONFIGURING A SINGLE VLAN ON A SINGLE PORT

In this example, you configure a NetScreen-5200 security device in L2V mode and the vsys “music”. The music vsys shares the music-untrust zone with the root system. You must import the VLANs to a vsys before they can be tagged.
1. Add a NetScreen-5000 security device in transparent mode running ScreenOS 5.0 L2V as the root system, then configure the network module:
   a. Double-click the device to open the device configuration. In the device navigation tree, select Network > Slot.
   b. Double-click slot 2 to display the slot configuration dialog box. For Card Type, select 5000-8G SPM.
   c. Click OK to save the slot configuration.

2. Create the vsys music. In the Device Manager, select Security Devices, then double-click the vsys music to open the vsys configuration.

3. Create two custom layer-2 zones on the vsys music:
   a. In the vsys configuration tree, select Network > Zones. Click the Add icon and select Security Zone. Configure the zone name as music-trust, then click OK.
   b. In the vsys configuration tree, select Network > Zones. Click the Add icon and select Security Zone. Configure the zone name as music-untrust, then click OK.

4. Import VLAN IDs from the root system to the vsys music:
   a. In the vsys navigation tree, select Network > Vlan > Import.
   b. Click the Add icon to display the New VLAN Import Entry. Configure the following, then click OK:
      - For Vlan ID Begin, enter 100.

Figure 91: Example Single Port L2V Configuration
5. Create a VLAN group on the vsys music. In the vsys navigation tree, select Network > Vlan > Group, then click the Add icon to display the New VLAN Group Entry. Configure the following:
   a. For Vlan Group Name, enter it_music.
   b. In the Setting Vlan Group area, click the Add icon to display the New Vlan Group Range. Configure the following, then click OK:
      - For Start Vlan ID, enter 100.
      - For End Vlan ID, enter 199.
   c. In the Binding Vlan Group to Port and Zone area, click the Add icon to display the New Vlan Group Port Settings. Configure the following, then click OK:
      - For Interface, select ethernet2/5.
      - For Zone, select music-trust.
   d. In the Binding Vlan Group to Port and Zone area, click the Add icon to display the New Vlan Group Port Settings. Configure the following, then click OK:
      - For Interface, select ethernet2/1.
      - For Zone, select music-untrust.

6. Create management interface for vsys music:
   a. In the vsys navigation tree, select Network > Interfaces, then click the Add icon and select VLAN Interface.
   b. Configure the following General Properties:
      - For Name, enter 199 (name appears as vlan199)
      - For Zone, select vlan.
      - For IP Address/Netmask, enter 1.0.1.199/24
      - Clear Manageable (deselect the checkbox).
   c. In the interface navigation tree, select Service Options. Select the Telnet, Ping, and Web, then click OK.

7. Configure zone firewall rules in a Security Policy for vsys music:
   a. Create a rule that permits HTTP traffic from music-untrust to music trust:
NetScreen-Security Manager 2005.3 Administrator's Guide

- For From zone, select music-untrust.
- For Source Address, select any.
- For To zone, select music-trust.
- For Destination Address, select any.
- For Service, select HTTP.
- For Action, select Permit.
- For Install On, right-click and select Select Target. In the Select Target Devices list, select the vsys music, then click OK.

b. Create a rule that denies all traffic from music-untrust to music trust:

- For From zone, select music-untrust.
- For Source Address, select any.
- For To zone, select music-trust.
- For Destination Address, select any.
- For Service, select any.
- For Action, select deny.
- For Install On, right-click and select Select Target. In the Select Target Devices list, select the vsys music, then click OK.

c. Create a rule that permits all traffic from music-trust to music untrust:

- For From zone, select music-trust.
- For Source Address, select any.
- For To zone, select music-untrust.
- For Destination Address, select any.
- For Service, select any.
- For Action, select Permit.
- For Install On, right-click and select Select Target. In the Select Target Devices list, select the vsys music, then click OK.

d. From the menu bar, select File > Assign Policy. In the Assign Policy to Devices list, select the vsys music, then click OK.
Configuring Certificates

Every security device supports the use of certificates to authenticate itself to outside parties. A digital certificate is an electronic means for verifying identity through a trusted third party, known as a Certificate Authority (CA). The CA is a trusted partner of the identity sending the digital certificate as well as the identity receiving it. To authenticate identity, the CA issues certificates, often with a set time limit. If you do not renew the certificate before the time limit is reached, the CA considers the certificate inactive. For example, a VPN member attempting to use an expired certificate is immediately detected (and rejected) by the CA.

You can use certificates to authenticate a VPN member (external device or security device), RAS users for a Group IKE ID, or SSL management of a security device. You must obtain and install the following certificates on the managed device before you can use certificates to authenticate the device:

- Configuring A Local Certificate—A local certificate authenticates the identity of the device on which it is installed.
- Configuring CA Certificates—A CA certificate authenticates a third party.
- Configuring CRLs (Optional)—A CRL ensures that expired certificates are not accepted.

**NOTE:** A CRL is optional; you do not need to obtain and install a CRL on the security device to use certificates.

When you import a security device that already has a local certificate, CA, and CRL installed, these certificates and lists are automatically imported as part of the device configuration when you add that device to the NetScreen-Security Manager system. However, to reuse the CA and CRL in other security devices, you must load the CA and CRL file directly into the management system (you cannot reuse a local certificate on another device). For details, see “Using Imported Certificates” on page 376.

**Using Self-Signed Certificates (ScreenOS 5.1 and Higher Only)**

For devices running ScreenOS 5.1 and higher, a self-signed certificate is automatically created each time the device powers on; you can use this self-signed certificate to authenticate the device for SSL management. Because this self-signed certificate is not authenticated by an external, third-party Certificate Authority, you cannot use it to authenticate a VPN member in an IKE VPN. A device running ScreenOS 5.1 and higher automatically creates the self-signed certificate upon reboot, so you do not need to configure a Generate Certificate Request to obtain it. However, if you delete the self-signed certificate for a device and do not want to reboot the device to obtain a new certificate, you can use the Generate Certificate Request procedure to prompt the device to re-generate the certificate. For details on configuring a Generate Certificate Request to obtain a self-signed certificate, see “Generating the Certificate Request” on page 370.

A self-signed certificate that was automatically generated by the device at startup has a certificate status of system. If you use the Generate Certificate Request to obtain a new self-signed certificate, the self-signed certificate has a certificate status of active.
Configuring A Local Certificate

A local certificate validates the identity of the security device. Each security device that performs authentication (in a VPN, for SSL management, for device administrators) must have a local certificate installed on the device. To view the available local certificates on a device, in the device navigation tree, select VPN Settings > Local Certificates.

To get a local certificate for a device, you must prompt the device to generate a certificate request (includes public/private key pair request) using the Generate Certificate Request directive. Depending on how you want to use the local certificate and the version of ScreenOS the device is running, you can configure a CA-signed local certificate or a self-signed local certificate:

- **Obtain a local certificate signed by a CA**—Use for devices running ScreenOS 4.0.x and 5.0, and for devices running ScreenOS 5.1 and higher that need to use a local certificate for authentication in an IKE VPN. When the device receives the prompt for a certificate request, it processes the request and returns the encrypted public key for the device. Using this encrypted public key, you can contact an independent CA (or use your own internal CA, if available) to obtain a local device certificate file (a .cer file). You must install this local certificate file on the managed device using NetScreen-Security Manager before you can use certificates to validate that device. Because the local certificate is device-specific, you must use a unique local certificate for each device.

- **Use the self-signed certificate**—Use for devices running ScreenOS 5.1 and higher that do not need to use the certificate for authentication in an IKE VPN. When configuring the request, select the option Create Self-Signed Certificate; when the device receives the certificate request, it processes the request and automatically add the certificate to the device. Because this certificate is both a local and CA certificate, you do not need to contact a CA.

For CA-signed local certificates, you can also use SCEP to configure the device to automatically obtain local certificate (and a CA certificate) from the CA directly.

Generating the Certificate Request

To send a certificate request prompt to the managed device, right-click the device and select Certificates > Generate Certificate Request. Enter the following information:

- **Name**—Enter the name of the certificate requestor; typically, this is the person who administrators the security device.

- **Phone**—Enter the telephone number of the certificate requestor.

- **Domain Component**—Enter one or more domain components for the certificate requestor. Multiple entries must be separated by commas.

- **Unit/Department**—Enter the unit or department of the certificate requestor.

- **Organization**—Enter the organization of the certificate requestor.

- **County/Locality**—Enter the county or locality of the certificate requestor.
- State—Enter the state of the certificate requestor.
- Country—Enter the country of the certificate requestor.
- E-mail—Enter the email address of the certificate requestor.
- IP Address—Enter the IP address of the certificate requestor.
- FQDN—Enter the fully-qualified domain name of the security device.
- Key Pair Type—Select RSA or DSA encryption.
- Key Pair Length—Select the key length: 512, 768, 1024, or 2048. Ensure that your Certificate Authority can support the key length you select. Key lengths greater than 1024 might require generation times longer than 10 minutes.
- Create Self-Signed Certificate (ScreenOS 5.1 and higher Only)—Select this option to use the self-signed certificate on a device running ScreenOS 5.1 and higher. Because the self-signed certificate is both the local certificate and the CA certificate, when this option is enabled the SCEP options are automatically disabled.
- Automatically Enroll—Select this option to use SCEP. The device automatically requests, receives, and installs the local certificate and the CA certificate locally. To use SCEP, configure the following defaults:
  - Certificate Authority. Select a preconfigured CA or use the default CA settings for the device.
  - E-mail request to. Provide the email address that receives the PKCS#10 file, which defines the syntax for certification requests.

Click OK to send the request prompt to the device. A Job Manager window appears to display job information and job progress. When the job is complete, the device public key appears in the Job window.

If you are obtaining the local certificate manually, you need the device public key to give to the CA. Copy and paste the information from the job window to a text file, or simply leave the job window open while you contact the CA.

If you are using SCEP to obtain a local certificate and a CA certificate, the device automatically sends its public key to the CA directly. When SCEP obtains both the local and CA certificate, the job completes. Close the Job Manager window, then check the status of certificates: open the device configuration and select VPN Settings > Local Certificates. The certificate status appears as active, indicating that the certificate file has been successfully installed on both the physical device and the management system (you might need to use the Refresh directive to prompt the UI to update the certificate status).
If you are using the self-signed certificate on a device running ScreenOS 5.1 and higher, the device automatically creates the certificate. A Job Manager window appears to display job information and job progress. When the job is complete, close the Job Manager window. To view the certificate, open the device configuration and select VPN Settings > Local Certificates. The certificate status appears as active, indicating that the self-signed certificate file has been successfully created and installed on both the physical device and the management system.

Obtaining and Installing the Local Certificate (CA or SCEP Only)
For CA-signed local certificates, after you prompt the device to generate the certificate request, the device creates the public/private key pair that is used to create the local certificate and returns the public key to the management system (the private key never leaves the device). During this time, the certificate status is key pair, meaning that a key pair exists but no certificate has been loaded.

After you obtain the local certificate, you must load the certificate into the management system using the NetScreen-Security Manager UI, then install the certificate on the managed device:

- For devices running ScreenOS 4.0.x and 5.0, you must install a TFTP server on the NetScreen-Security Manager Device Server. The Device Server automatically uses TFTP to load the certificate onto your managed devices. For more information on creating a TFTP server on the Device Server, see the NetScreen-Security Manager 2005.3 Installer’s Guide.

- For devices running ScreenOS 5.1 and higher, the Device Server automatically uses Secure Server Protocol (SSP) to load firmware onto your managed devices. SSP is the protocol used for the management connection between the physical device and the NetScreen-Security Manager Device Server.

After the certificate is installed on the device, the certificate is known as active. To view the current status of your certificate requests, open the device configuration and select VPN Settings > Local Certificates:

- Before the certificate is fulfilled, the certificate status appears as key pair, indicating a public/private key pair exists but the certificate file does not yet exist on both the physical device and the management system.

- After the certificate is fulfilled, the certificate status appears as active, indicating that the certificate file has been successfully installed on both the physical device and the management system.

NOTE: Any time you need to move information from the physical device to the management system, you are using a Refresh directive; when you need to move information from the management system to the physical device, you are using an Update directive.
Installing the Local Certificate Using SCEP

If you used SCEP for automatic enrollment, the device contacts the specified CA and obtains a local and CA certificate. After the device has installed the certificate, refresh the NetScreen-Security Manager device configuration for that device to view the new certificate information:

1. Right-click the device and select Certificates > Refresh Local Certificates. This directive uses the information on the physical device to refresh the information on the management system.

2. Open the device configuration to view the local certificates in VPN Settings > Local Certificates. The certificate status appears as active, indicating that the certificate file has been successfully installed on both the physical device and the management system.

Installing the Local Certificate Manually

If you did not use SCEP, you must manually contact your CA and use the device public key to create a local device certificate. After you have obtained the local certificate (.cer) file from your CA, install that certificate on the device:

1. Right-click the device and select Certificates > Update Fulfilled Certificate. This directive uses the information in the management system to update the information on the physical system.

2. Load the certificate file and click OK to install the local certificate on the device. A Job Manager window appears to display job information and job progress. When the job is complete, close the Job Manager window.

3. To view the local certificate, open the device configuration and select VPN Settings > Local Certificates. The certificate status appears as active, indicating that the certificate file has been successfully installed on both the physical device and the management system.

NOTE: For devices running ScreenOS 4.0.x and 5.0, you must install a TFTP server on the NetScreen-Security Manager Device Server. The Device Server automatically uses TFTP to load the local certificate onto your managed devices. For more information on creating a TFTP server on the Device Server, see the NetScreen-Security Manager 2005.3 Installer’s Guide.

For devices running ScreenOS 5.1 and higher, the Device Server automatically uses Secure Server Protocol (SSP) (the protocol used for the management connection) to load the local certificate.
Configuring CA Certificates

A CA certificate validates the identity of the third party CA that issued the local device certificate. To view the available CA certificates on a device, in the device navigation tree, select VPN Settings > CA Certificates.

NOTE: If you are using a self-signed certificate, you do not need to contact a CA. The self-signed certificate on the device is issued and signed by the same entity (the device), so the issuer and the subject of the certificate are the same. However, because this self-signed certificate is not authenticated by an external, third-party Certificate Authority, you cannot use it to authenticate a VPN member in an IKE VPN.

To obtain a CA certificate file (.cer), contact the CA that issued the local certificate, then use this file to create a Certificate Authority object. You must install this CA certificate on the managed device using NetScreen-Security Manager before you can use certificate to validate that device in your VPN. Because the CA certificate is an object, however, you can use the same CA for multiple devices, as long as those devices use local certificates that were issued by that CA.

You can also use SCEP to configure the device to automatically obtain a CA certificate at the same time it receives the local certificate. For details on configuring a certificate authority object, see “Configuring Certificate Authorities” on page 521.

The following sections detail how to add a CA certificate to a device using SCEP or manually.

Obtaining and Installing a CA Certificate Using SCEP

If you used SCEP to obtain a local certificate for the device, the CA certificate was automatically downloaded and installed on the device at the same time as the local certificate. However, because the management system does not know about the CA certificate, you must refresh the CA information:

1. Right-click the device and select Certificates > Refresh CA Certificates. This directive uses the information on the physical device to refresh the information on the management system.

2. Open the device configuration to view the CA certificates in VPN Settings > CA Certificates.

Obtaining and Installing a CA Certificate Manually

If you did not use SCEP, you must manually contact your CA, obtain a CA certificate, and create a Certificate Authority Object. Then, add the CA certificate to the device and install it on the device:

1. Open the device configuration and select VPN Settings > CA Certificates. Click the Add icon and add the Certificate Authority object. Close the device configuration.
2. Right-click the device and select Certificates > Update CA Certificate. This directive uses the information in the management system to update the information on the physical system. A Job Manager window appears to display job information and job progress.

NOTE: For devices running ScreenOS 4.0.x and 5.0, you must install a TFTP server on the NetScreen-Security Manager Device Server. The Device Server automatically uses TFTP to load the CA certificate onto your managed devices. For more information on creating a TFTP server on the Device Server, see the NetScreen-Security Manager 2005.3 Installer’s Guide.

For devices running ScreenOS 5.1 and higher, the Device Server automatically uses Secure Server Protocol (SSP) (the protocol used for the management connection) to load the CA certificate.

3. When the job is complete, close the Job Manager window.

To view CA certificate, open the device configuration and select VPN Settings > CA Certificates.

**Configuring CRLs**

A Certificate Revocation List (CRL) identifies invalid certificates. To view the available CRLs on a device, in the device navigation tree, select VPN Settings > CRLs. To obtain a CRL file (.crl), contact the CA that issued the local certification and CA certificate for the device, then use this file to create a Certificate Revocation List object.

You must install the CRL on the managed device using NetScreen-Security Manager before you can use a CRL to check for revoked certificates in your VPN. Because the CRL is an object, however, you can use the same CRL for multiple devices, as long as those devices use local and CA certificates that were issued by that CA. After you have received a CRL, you can use the CRL object in your VPN. For details on configuring a certificate revocation list object, see “Configuring CRL Objects” on page 524.

You must manually contact your CA, obtain a CRL, and create a Certificate Revocation List Object. Then, add the CRL to the device and install it on the device:

1. Open the device configuration and select VPN Settings > CRLs. Click the Add icon and add the Certificate Revocation List object. Close the device configuration.
2. Right-click the device and select Certificates > Update CRL. This directive uses the information in the management system to update the information on the physical system. A Job Manager window appears to display job information and job progress.

NOTE: For devices running ScreenOS 4.0.x and 5.0, you must install a TFTP server on the NetScreen-Security Manager Device Server. The Device Server automatically uses TFTP to load the CRL onto your managed devices. For more information on creating a TFTP server on the Device Server, see the NetScreen-Security Manager 2005.3 Installer’s Guide.

For devices running ScreenOS 5.1 and higher, the Device Server automatically uses Secure Server Protocol (SSP) (the protocol used for the management connection) to load CRLs.

3. When the job is complete, close the Job Manager window.

To view CRL, open the device configuration and select VPN Settings > CRL.

Using Imported Certificates

If you imported a security device that already has a local certificate, CA, and CRL, these objects are automatically imported when you add that device to the NetScreen-Security Manager system. Imported objects use the default name of <CN>_<timestamp>.

However, to reuse the CA and CRL objects in other security devices, you must load the CA and CRL file directly into the management system:

- To load a CA file (.cer) into the management system, open the imported CA object in Object Manager and use the Load Certificate option. After loading the CA, verify the status of the certificate appears as Loaded.
- To load a CRL file (.crl) into the management system, open the imported CRL object in Object Manager and use the Load CRL option. After loading the CRL, verify the status of the CRL appears as Loaded.

After the CA certificate and CRL files have been loaded, you can use those CA and CRL objects in other devices.

Configuring PKI Defaults

You can configure default PKI settings for each security device that define how that device handles certificates. When configuring a VPN that includes the device, you can use these default settings.

In device configuration tree, select VPN Settings > Defaults > PKI Settings to display the default PKI settings. First, configure the source interface for PKI Traffic. The source interface is the interface on the device that sends the certificate request to the CA.

Configuring X509 Certificates

Configure the following X509 certificate settings:
Email Destination for the PKCS#10 File—Provide the email address that receives the PKCS#10, which defines the syntax for certification requests.

Select raw common name—Select this option to use only one CN field in the certificate CN in SCEP certificate request. Some certificate authorities support a single CN filed in the certificate DN, when responding to a SCEP request. When enabled, the CN field contains the value of certificate name when you set DN.

Configuring Revocation
Revocation settings define how and when certificates are revoked. You might want to revoke a certificate that you suspect has been compromised or when a certificate holder leaves a company. You can revoke the certificate manually, or use CRL or OCSP to automatically check for revoked certificates.

X.509 Certificate Path Validation Level. X509 contains a specification for a certificate which binds an entity’s distinguished name to its public key through the use of a digital signature.

- Full. Use full validation to validate the certificate path back to the root.
- Partial. Use partial validation to validate the certificate path only part of the way to the root.

Revocation Check. Select or clear revocation checking for certificates:
- Check for revocation. Select this option to enable revocation checking.
- Do not check for revocation. Select this option to disable revocation checking.

Revocation Checking Method—If you enabled revocation checking, you can select the checking method to use. If you did not enable revocation checking, these fields are unavailable.

- CRL. Use a Certificate Revocation List when you want to keep a local copy of the revoked certificates on the managed device. This method enables you to check for revoked certificates quickly.
- OCSP. Use the Online Certificate Status Protocol when you want the managed device to access a remote OCSP server to check for revoked certificates. Because the OCSP server dynamically updated their list of revoked certificates, this method provides the most up-to-date information.
- Best Effort—Select this option to check for revocation accept the certificate if no revocation information is found.

CRL Settings—Configure the default setting for the Certificate Revocation List.
- URL address. Provide the URL address of your internal LDAP server that provides the CRL.
- LDAP server. Provide the IP address of the external LDAP server that manages the CRL.
- Refresh Frequency. Select the frequency that the device contacts the CA to obtain a new CRL list: Daily, Weekly, or Monthly.

- OCSP—Configure the Online Certificate Status Protocol to dynamically check for revoked certificates.

- Certificate Verification. Select the CA certificate used to verify the signature on the OCSP response.

- No revoke status check for CA delegated signing cert. Select this option if you do not want the original CA certificate to verify the validity of the CA delegated OCSP signing certificate. When enabled, the validity of the OCSP signing certificate is verified by original CA certificate.

- URL of OCSP Responder. Provide the URL address of the OCSP server.

Configuring SCEP
Alternatively, you can use Simple Certificate Enrollment Protocol (SCEP) to get a local certificate automatically. To enable SCEP for a managed device, configure the default PKI settings for SCEP:

- CA CGI—Enter the URL address of the Certificate Authority Certificate Generation Information.

- RA CGI—Enter the URL address of the Registration Authority Certificate Generation Information that the security device contacts to request a CA certificate.

- CA IDENT—Enter the name of the certificate authority to confirm certificate ownership.

- Challenge—Enter the challenge word(s) sent to you by the CA that confirm the security device identity to the CA.

- CA Certificate Authentication—Configure the default method for obtaining CA certificates:
  - Auto. Select this option for CA certificates retrieved through SCEP.
  - Manual. Select this option for CA certificates retrieved manually.

- Polling Interval. NetScreen-Security Manager searches the list of the pending certificates based on this setting and records the time due for the first pending certificate. This process repeats 48 times; after that time, pending certificates can be polled only manually. When polling succeeds, NetScreen-Security Manager removes the pending certificate from the pending certificate list and schedules no new polling.
  - Poll. When enabled, you can configure the number of minutes between polls.
  - Do not poll. Use this option to disable automatic polling.

- Certificate Renewal—Define the number of times a certificate can be renewed.
Configuring NSRP Clusters

An NSRP cluster consists of two security devices that enforce the same Security Policy and share the same configuration settings. When you assign a security device to an NSRP cluster, any changes you make to the configuration on one member of the cluster propagate to the other. Members of the same NSRP cluster maintain identical settings for policies and policy objects (such as addresses, services, VPNs, users, and schedules) and system parameters (such as settings for authentication servers, DNS, SNMP, syslog, and so on).

The following sections detail NSRP configuration:

- About NSRP Clusters
- Creating an NSRP Cluster
- Active/Passive Configurations
- Active/Active Configurations
- Synchronizing Configurations
- Forcing VSD Group Member State
- Configuring Monitoring (For Failover)
- Configuring Vsys Clusters

About NSRP Clusters

Before two security devices can provide redundant network connectivity, you must group them in the same NSRP cluster. In an NSRP cluster, one device acts as a master and the other as its backup:

- In **active/passive** configurations, the master handles all firewall and VPN activities while the backup waits to take over when the master steps down. You can configure the cluster in active/passive operation when the interfaces are in transparent, NAT, or route mode:

  - **Transparent Mode.** When interfaces are in Transparent mode, the device operates at Layer 2. The security zone interfaces do not have IP addresses, and the security device forwards traffic like a Layer 2 switch. To manage a backup device, you use the manage IP address that you set on the VLAN1 interface.

  - **NAT or Route Mode.** When interfaces are in NAT or Route mode, the security device operates at Layer 3 in the OSI model. The security zone interfaces have IP addresses, and the device forwards traffic like a Layer 3 router. To manage a backup device, you must use the manage IP address that you set per security zone interface; you cannot set a manage IP address on a VSI for any VSD group except VSD group 0.
In *active/active* configurations, you create two virtual security devices (VSD) groups for the cluster: One device acts as the master of one VSD group, while the other device acts as the backup for the same group. In the other VSD group, the device roles are reversed: Each device is the master of one VSD group and the backup in the other VSD group. You can configure the cluster in *active/active* operation when the interfaces are in NAT or route mode. The security device operates at Layer 3 in the OSI model. The security zone interfaces have IP addresses, and the device forwards traffic like a Layer 3 router. To manage a backup device, you must use the manage IP address that you set per security zone interface; you cannot set a manage IP address on a VSI for any VSD group except VSD group 0.

Because of the sensitive nature of NSRP communications, you can secure all NSRP traffic through encryption and authentication. For encryption and authentication, NSRP supports the DES and MD5 algorithms respectively. However, if the HA cables run directly from one security device to another (that is, not through a switch forwarding other kinds of network traffic), it is unnecessary to use encryption and authentication.

In addition to NSRP clusters, which propagate configurations among group members and advertise each members’ current VSD group states, you can configure the devices as members in an RTO mirror group, which maintains the synchronicity of run-time objects (RTOs) between a pair of devices. When the master steps down, the backup can immediately assume mastership with minimal service downtime by maintaining all current sessions.

For more detailed explanations of NSRP, see the “NSRP” volume in the NetScreen Concepts & Examples ScreenOS Reference Guide for ScreenOS 4.0.0 or the “High Availability” volume in the NetScreen Concepts & Examples ScreenOS Reference Guide.

### Creating an NSRP Cluster

To create an NSRP cluster, either by importing or modeling, first add the cluster to NetScreen-Security Manager. In the Device Manager, click the Add icon and select Cluster. Follow the directions in the Add Device wizard to add the cluster. When you select the device model and ScreenOS version, remember that all devices in a cluster must be the same device model and run the same ScreenOS version.

Next, add devices to the cluster: Right-click the cluster and select New > Cluster Member. Follow the directions in the Add Device wizard to import or model the cluster member.

| NOTE: | When importing cluster device members, ensure that their device configurations are in sync (errors can occur in the import process if you attempt to import out-of-sync configurations). |

Finally, configure the cluster and the cluster members (you must configure cluster members from within the cluster itself). To configure a cluster member, open the Cluster device configuration and select Members in the Cluster navigation tree. Double-click the cluster member you want to configure to open its device configuration, then make your changes.
Most settings entered on one device in a cluster propagate to the other device, however, some configurations, such as setting NSRP authentication and encryption passwords, do not propagate. If you are using NSRP authentication and encryption passwords in the cluster, you need to configure the same information on all devices in the cluster.

For step-by-step instructions on adding member devices to a cluster, see the NetScreen-Security Manager Online Help topic “Configuring NSRP Clusters”.

For more information about configurations that do not propagate, see the “NSRP” volume in the JNetScreen Concepts & Examples ScreenOS Reference Guide for ScreenOS 4.0.0 or the “High Availability” volume in the NetScreen Concepts & Examples ScreenOS Reference Guide.

**Active/Passive Configurations**

To ensure continuous traffic flow, you can enable and configure two security devices in a redundant cluster, with one device acting as a master and the other as its backup. The master propagates all its network and configuration settings and the current session information to the backup. Should the master fail, the backup is promoted to master and takes over the traffic processing.

In this example, you want to configure two NetScreen-208 security devices, Corporate A and Corporate B, in an NSRP cluster. Both device are running ScreenOS 5.x. Using a cable, connect the ethernet7 interfaces of both devices, then use another cable to connect the ethernet8 interfaces. Next, add the cluster and cluster member to NetScreen-Security Manager. When the devices become members of the NSRP cluster, the IP addresses of their physical interfaces automatically become the IP addresses of the Virtual Security Interfaces (VSIs) for VSD group ID 0. Each VSD member has a default priority of 100, the device with the higher unit ID becomes the VSD group master.

**NOTE:** When using a PPPoE connection to an ISP for Internet access, you can bind the PPPoE instance to a VSI interface. In the event of failover, this configuration enables the new master to use the same IP and PPPoE connection as the previous master. For details, see “Configuring PPPoE” on page 282.

By default, the two cluster members are configured as active/passive after you add them to the cluster object. NetScreen-Security Manager automatically creates VSD group 0 and transforms physical interfaces into Virtual Security Interfaces (VSIs) for VSD group 0.

To configure an active/passive cluster, you must:

1. Cable two security devices together.
2. Select automatic RTO synchronization
3. Select the ports that you want the devices to monitor, so that if they detect a loss of network connectivity on one of the monitored ports, the device fails over.

**EXAMPLE: CONFIGURING NSRP FOR AN ACTIVE/PASSIVE CONFIGURATION**

In this example, you want to configure two NetScreen-208 security devices, Corporate A and Corporate B, in an NSRP cluster. Both device are running ScreenOS 5.x. Using a cable, connect the ethernet7 interfaces of both devices, then use another cable to connect the ethernet8 interfaces. Next, add the cluster and cluster member to NetScreen-Security Manager. When the devices become members of the NSRP cluster, the IP addresses of their physical interfaces automatically become the IP addresses of the Virtual Security Interfaces (VSIs) for VSD group ID 0. Each VSD member has a default priority of 100, the device with the higher unit ID becomes the VSD group master.
Finally, configure the cluster:

- Bind ethernet7 and ethernet8 to the HA zone. By default, ethernet8 is bound to the HA zone, so you only need to bind it to the HA zone if you have previously bound it to a different zone.

- Set manage IP addresses for the Trust zone interfaces on both devices.

- Configure monitoring on ethernet1 and ethernet3, so that loss of network connectivity on either of those ports triggers a device failover.

- Select automatic synchronization of RTOs.

Figure 92: Example of NSRP Active/Passive Configuration

1. Create the Cluster:
   
   a. In the navigation tree, select Device Manager > Security Devices. Click the Add icon and select Cluster. Configure the following, then click OK:

   - For Cluster Name, enter Corporate.
   - For Color, select cyan.
   - For Physical Choice, select ns208.
   - For OS Version, select 5.0.
   - Ensure that Transparent Mode is not enabled (unchecked).
For License Model, select Advanced.

b. Add the following two cluster members to the cluster: Corporate A, Corporate B. Choose Model when adding each device.

2. Configure the HA interfaces for the cluster.
   b. For Zone, select HA, then click OK to save your changes.
   d. Ensure that the zone name HA, then click OK to save your changes.

3. Configure the Untrust interface for the cluster:
   b. For Zone, select Untrust.
   c. For IP address and netmask, enter 210.1.1.1/24.
   d. Click OK to save your changes.

4. Configure the Trust interface for the cluster:
   b. For Zone, select Trust.
   c. For IP address and netmask, enter 10.1.1.1/24.
   d. Ensure that the interface mode is NAT, then click OK to save your changes.
   e. Click Apply to apply all previous changes to the cluster members.

5. Configure the Manage IP and Monitoring for Corporate A:
   a. In the cluster navigation tree, select Members. Double-click Corporate A to open its device configuration.
   b. In the device navigation tree, select Network > Interface and double-click ethernet 3. The General Properties screen appears.
   c. For Manage IP, enter 10.1.1.20, then click OK to save your changes.
   d. In the device navigation tree, select Monitoring > Whole Box Monitoring, then select the Monitor Interface tab.
e. Click the Add icon to display the new monitor interface dialog box. Select ethernet1, leave the default weight of 255, and click OK to save your changes.

f. Click the Add icon to display the new monitor interface dialog box. Select ethernet3, leave the default weight of 255, and click OK to save your changes.

g. Click OK to close the device configuration for Corporate A.

6. Configure the Manage IP for Corporate B:

a. In the cluster navigation tree, select Members. Double-click Corporate B to open its device configuration.

b. In the device navigation tree, select Network > Interface and double-click ethernet 3. The General Properties screen appears.

c. For Manage IP, enter 10.1.1.21, then click OK to save your changes.

d. In the device navigation tree, select Monitoring > Whole Box Monitoring, then select the Monitor Interface tab.

e. Click the Add icon to display the new monitor interface dialog box. Select ethernet1, leave the default weight of 255, and click OK to save your changes.

f. Click the Add icon to display the new monitor interface dialog box. Select ethernet3, leave the default weight of 255, and click OK to save your changes.

g. Click OK to close the device configuration for Corporate B.

7. Configure the NSRP settings:

a. In the cluster navigation tree, select NSRP.

b. Select RTO Sync.

8. Click OK to save your changes to the cluster and cluster members.

Active/Active Configurations

On a security device in Route or NAT mode, you can configure both devices in a redundant cluster to be active, sharing the traffic distributed between them by routers with load-balancing capabilities running a protocol such as the Virtual Router Redundancy Protocol (VRRP).

Using NSRP, you create two virtual security devices (VSD) groups, each with its own virtual security interfaces (VSIs). For example, Device A acts as the master of VSD group 1 and as the backup of VSD group 2. Device B acts as the master of VSD group 2 and as the backup of VSD group 1. Devices A and B each receive 50% of the network and VPN traffic. Should device A fail, device B becomes the master of VSD group 1, as well as continuing to be the master of VSD group 2, and handles 100% of the traffic.
Although the total number of sessions divided between the two devices in an active/active configuration cannot exceed the capacity of a single security device (otherwise, in the case of a failover, the excess sessions might be lost), the addition of a second device doubles the available bandwidth potential. A second active device also guarantees that both devices have functioning network connections.

To configure an active/active cluster, you must configure a second VSD group:

1. Double-click the cluster to open the cluster configuration. In the cluster navigation tree, select Members.
2. In the VSD definitions area, click the Add icon to display the Add VSD dialog box.
3. Select a value other than 0, then click OK to save the new VSD. The VSD you added appears in the VSD Definitions list.
4. Click OK to save your changes to the cluster.

The VSD group member with the priority number closest to 0 becomes the master. (The default is 100.) If two devices have the same priority value, the device with the lowest MAC address becomes master.

**Synchronizing Configurations**

After you add new members to an NSRP cluster, you must synchronize the configuration and files from one device to another.

To synchronize configurations:

1. In the Device Manager, double-click the cluster to open the cluster configuration.
2. In the cluster navigation tree, select NSRP Directives > Flash Sync.
3. Select the device that will be used to synchronize the other device and click Perform Sync. The device that has been synchronized is automatically rebooted to activate the new configuration.
4. Click OK to save your changes to the cluster.

**Synchronizing the Virtual Router**

You can configure the virtual router information for the cluster or cluster members. For devices running 4.0.x or 5.0, you must configure the virtual router settings at the system level (the cluster).

For devices running ScreenOS 5.1 and higher, you can configure the virtual router setting at the system level (the cluster) or at the local level (cluster member). By default, cluster members automatically use the virtual router settings of the cluster. To use different vrouter settings for each cluster member, you must disable NSRP configuration synchronization for the vrouter at the system level:

1. In the main navigation tree, select Device Manager > Security Devices, then double-click the cluster to open the cluster configuration.
2. In the cluster navigation tree, select Network > Virtual Router. Double-click the trust-vr virtual router. The General Properties screen appears.

3. Disable Enable NSRP Configuration Sync for Vrouter (clear the checkbox), then click Apply to save your changes to the cluster.

4. In the cluster navigation tree, select Members and double-click a cluster member device to open the device configuration. Edit the virtual router settings as desired.

NOTE: The Enable NSRP Configuration Sync setting does not affect the Vrouter ID. The Vrouter ID setting is always configured at the local level (cluster member).

5. Click OK to save your changes to the cluster member, then click OK to save your changes to the cluster.

Synchronizing Run-Time Objects (RTOs)

After synchronizing the configurations and files, you can then synchronize the run-time objects (RTOs). RTOs are code objects created dynamically in memory during normal operation. Some examples of RTOs are session table entries, ARP cache entries, DHCP leases, and IPSec security associations (SAs). In the event of a failover, the new master must maintain the current RTOs to avoid service interruption.

To ensure session backup, the members of an NSRP cluster backup the RTOs using an RTP mirror group. An RTO mirror group is a pair of security devices that pass RTOs unidirectionally from a sender to a receiver. You can also create a second mirror group (with a different group ID from the first group) for the same devices but reverse the roles of sender and receiver. Working together, each member backs up the RTOs from the other, which permits RTOs to be maintained should the master of either VSD group in an active/active HA scheme step down.

After you add the cluster members, you can configure RTO synchronization to enable each member to send and receive RTOs. However, by default, NSRP cluster members do not synchronize their configurations before synchronizing RTOs; before enabling RTO synchronization, you must first synchronize the configurations between the cluster members. Unless the configurations on both members in the cluster are identical, RTO synchronization might fail.

Forcing VSD Group Member State

If necessary, for troubleshooting or maintenance, you can force a device to assume a new mode (master, backup, or ineligible) in a specified VSD group. To do this:

1. In the Device Manager, double-click the cluster to open the cluster configuration.

2. In the cluster navigation tree, select NSRP Directives > Exec Mode.

3. Select the device that will assume a new role, then click Exec Mode. The Mode Selection dialog box appears.

4. Select the mode that the device is to assume:
Configuring NSRP Clusters

- **Master**—The VSD group member processes traffic sent to the VSI.

- **Backup**—The VSD group member becomes the master should the current master step down. The election process uses device priorities to determine which member to promote. When electing a new master, an RTO peer has precedence over any other VSD group member, even if that member has a better priority rating.

- **Ineligible**—The VSD group member cannot participate in the election process. The preempt option must be enabled on the master device for this option to appear.

5. Click OK to save your changes.

**EXAMPLE: CHANGING VSD GROUP MEMBER STATE**

In this example, you change the VSD group member states.

1. In the cluster navigation tree, select NSRP Directives > Exec Mode.
   - Select Office A, then click Exec Mode. Configure as master of VSD group 0.
   - Select Office B, then click Exec Mode. Configure as master of VSD group 1.

Both configurations are shown below:

Figure 93: Configuring VSD Group Masters
2. Click OK to save your changes to the cluster.

### Configuring Monitoring (For Failover)

You can configure NSRP to detect interface and zone failures on a device or VSD group. When one or more monitored objects on a device or VSD group fail, the master device in the cluster or VSD group can fail over to the backup device or VSD group.

To control when the device or VSD group fails over, you configure the device to monitor specific objects.

**NOTE:** Each Vsys cluster device can see all VSDs in the cluster, even VSDs that the Vsys cluster device does not use. This means that you could configure a Vsys cluster device to monitor a VSD group that the device does not use. If this monitored VSD group failed, the Vsys cluster device that does use that VSD group would failover—not the Vsys cluster device that was configured to monitor the VSD group.

For each device or VSD group, you can monitor:

- **Specific target IP addresses**—the device sends ping or ARP requests to up to 16 specified IP addresses at specified intervals and then monitors responses from the targets. All the IP addresses configured on the device or for a specified VSD group constitute a single monitored object.
- **Physical interfaces**—The device uses NSRP to check that the physical ports are active and connected to other devices.
- **Zones**—The device uses NSRP to check that all physical ports in a zone are active.

For each monitored object, you must configure a threshold, which is the total weight of failed monitored objects required to cause the device or VSD group to step down as master. If the cumulative weight of the failures of all monitored objects exceeds the monitored object failure threshold and the monitor threshold, then the device or VSD group fails over to the backup device or VSD group. You can set the monitored object failover threshold at any value between 1 and 255. The default threshold is 255.

You must also configure a failure weight, which is the weight that the failure of the monitored object contributes towards the device or VSD group failover threshold, which is known as the monitor threshold. You can set the object failure weight at any value between 1 and 255. The default failure weight for monitored objects is 255. If you want to monitor an object but do not want the failure of the object to affect failover of the device or VSD group, set the failure weight of the object to 0 (all failures are logged, even if the failure weight of the object is 0).
Configuring Track IPs

For tracked IP addresses, you specify individual IP addresses, how they are to be monitored, what constitutes the failure of each tracked IP address (the threshold), and the weight that each failed address carries. When IP tracking is enabled, the device sends a request on the selected interface to target IP addresses at specified intervals, then monitors the targets for responses. If the device does not receive a response from a target for a specified number of times, the device considers that IP address to be unreachable. You configure the threshold (the number of acceptable consecutive response failures) for each IP address within the IP Option dialog box. The default threshold for each IP address is 3; acceptable values are 1 to 200.

If the device does not receive a response from a specified number of targets, the device can deactivate routes associated with the selected interface. This threshold, known as the failure threshold, is the sum of the weights of all failed tracked IP addresses required for the tracked IP object to be considered failed. You configure the interface threshold (the total weight of the cumulative failed attempts) in the Track IP tab. The default is 1; acceptable values are 1 to 255, which means a failure to reach any configured tracked IP address causes routes associated with the interface to be deactivated.

For each interface, you can configure up to four IP addresses to track. The tracked IP addresses do not have to be in the same subnetwork as the interface.

NOTE: A single device can track 64 IP addresses. This total includes all track IP addresses for interface-based IP tracking and for NSRP-based IP tracking at the root level and vsys level.

Configuring Interface Monitoring

The device uses NSRP to check that the physical ports are active and connected to other network devices. When the port is inactive, the device considers the interface failed.

The process for adding an interface to monitor is as follows:

- **Edit the cluster by selecting and editing its members.**
- **Select Monitoring > Whole Box Monitoring.**
- **Use the Monitor Interface tab to select all the interfaces that need to be monitored and define the weightage for each interface.** You can assign a weight to each interface in the device or VSD group to indicate the importance of that interface. The higher the weight, the faster the failover threshold is met. For example, if the untrust interface is more important than the management interface, assign the untrust interface a higher weight than the management interface.

For example, when using two VSD groups (VSD 1 and VSD 2) configured on two devices (device A and device B), if a port on a master device in a VSD group fails, you can configure VSD 1 to failover from the primary VSD group on device A to the backup VSD group on device B. VSD 2 remains active on device A.
Configuring Zone Monitoring

The device uses NSRP to check that all physical ports in a zone are active and connected to other network devices. When all ports within the zone are inactive, the device considers the zone failed.

You can assign a weight to each zone in the device or VSD group to indicate the importance of that zone. The higher the weight, the faster the failover threshold is met. For example, if the DMZ zone is more important than the trust zone, assign the DMZ zone a higher weight than the trust zone.

All interfaces bound to the monitored zone must fail before the device considers the zone down. Specifically:

- If a monitored zone has multiple interfaces, but only one interface in the zone is active, the device considers the zone active.
- If a monitored zone has a single interface bound to it and that interface is failed, the device considered the zone as failed.
- If a monitored zone has no interfaces bound to it, the zone cannot fail.
- If you unbind a downed interface from a zone that contains only that interface, the device no longer considers the zone failed. Similarly, if you unbind an active interface from a monitored zone where the remaining interfaces are down, the device considers the zone failed.

Configuring Monitor Threshold

The monitor threshold is the failure threshold for the device or VSD group. All failure weights for all monitored objects in the device or VSD group contribute to the monitor threshold when a failure occurs; if the total sum of these failure weights meets or exceeds the monitor threshold, the device or VSD group fails over.

Alternatively, even if all IP addresses, interfaces, and zone fail in the device or VSD group, if the sum of their failure weights does not meet or exceed the monitor threshold, the device or VSD group does not fail over to the backup VSD group. To ensure that the device or VSD group fails over at the appropriate time, configure the failure weights of each monitored object in relation to the monitor threshold.

Configuring Vsyst Clusters

A vsys cluster is a vsys device that has a cluster as its root device.

To enable failover from one virtual system to another, you must create a virtual system interface (VSI) for each virtual system. A logical entity at layer 3 that is linked to multiple layer 2 physical interfaces in a VSD group. The VSI binds to the physical interface of the device acting as master of the VSD group. The VSI shifts to the physical interface of another device in the VSD group if there is a failover and it becomes the new master.

- Trust zone VSIs—each vsys has its own trust zone vsi by default. All Trust zone virtual system VSIs must be in different subnets.
Untrust zone VSIs—you can configure each vsys to use its own Untrust zone VSI or share the Untrust zone VSI from the root device. When virtual systems have their own Untrust zone VSIs, the VSIs must be in different subnets from each other and from the Untrust zone VSI at the root level.

After creating VSI, you must also create VSD groups to contain these VSIs.

### Exporting and Importing Device Configurations

Use the Export Device Config To File directive to export an existing configuration on a security device(s) to a file.

**To Export a Device Config To File**

1. From the Device Manager, select a security device.
2. From the Device menu, select **Device > Configuration > Export Device Config To File**.
3. Select a security device(s). A Job Information window appears displaying the status of the export process.

After the export has completed, you can then use the Import Device Config to File function to import that configuration to a security device.

**NOTE:** You cannot import a device configuration file that was exported from a previous version of NetScreen-Security Manager.
Chapter 6
Updating Devices

This chapter details how to update the running configuration (the configuration on the security device) with the modeled configuration (the configuration in the Juniper Networks NetScreen-Security Manager UI). In addition to covering the basic update process, this chapter also details the events that can require you to update your device, as well as NetScreen-Security Manager tools that help you to track, verify, and preview the update process.

After you model or make changes to a device configuration in the NetScreen-Security Manager UI, you must install that device configuration on the physical Juniper Networks security device before those changes can take effect. For devices running ScreenOS 5.x, NetScreen-Security Manager supports atomic configuration, a fail-safe feature that ensures successful updates occur without errors or the update is not performed. Atomic configuration is always enabled and occurs automatically when a device update causes the device to lose its connection to the management server.

The following sections are in this chapter:

- About Updating
- Knowing When to Update
- Using Preview Tools
- Delta Configuration Summary Example
- Performing an Update
- Tracking Device Updates
About Updating

When you updated a managed device, you are modifying the running device configuration (the configuration currently installed on the physical device) with the modeled device configuration (the configuration currently modeled in NetScreen-Security Manager).

You can update a single device, multiple devices, vsys devices, clusters, and/or device groups simultaneously. For example, if you have created a device group that includes only NetScreen-5GT devices, you can update the entire device group in a single update procedure. During the update, NetScreen-Security Manager displays the progress of the update on each individual device so you can see exactly what is happening. Simultaneous updating also reduces downtime to unaffected devices and areas of your network.

Updating a device is a simple three-step process.

1. Ensure that you have configured the device correctly, created and assigned a policy to the device, and have established a connection between the device and the management server.

2. From the menu bar, select Devices > Configuration > Update Config. NetScreen-Security Manager displays the Update Devices dialog box.
   - All connected and managed device appear in the device list. Modeled devices, or devices awaiting import for the first time do not appear.
   - For devices running ScreenOS 5.1 or higher, the configuration status also appears next to the device name. For more details on configuration states, see “Configuration Status” on page 396.

3. Select the devices or device groups you want to update and click OK. NetScreen-Security Manager updates the selected devices or device groups with the modeled configuration.

NetScreen-Security Manager uses centralized control and tracking to indicate when you need to update a device, and to follow the progress of the device configuration you are updating. Before updating your managed devices, you can use other NetScreen-Security Manager modules and tools to identify devices that need to be updated, validate their modeled configurations, and preview how those devices accept the new configuration. After updating, you can use those same tools to verify a successful update. These tools include:
   - Audit Log Viewer—This NetScreen-Security Manager module records changes made to a device configuration. The audit log entry also details the administrator performed the change, when the change was updated on the device, and a history of change details.

NOTE: Although atomic configuration provides fail-safe methods of protecting your ScreenOS 5.x devices from invalid configurations, you should be confident about the modeled configuration before updating the device.

390  About Updating
Report Manager—This NetScreen-Security Manager module collects data from traffic logs on various events that occur over your network and provides a visual representation of them. You can customize reports to display and filter parameters.

Configuration Summaries—These tools provide a preview of the modeled configuration, enabling you to compare it with the configuration that is running on the device. Use configuration summaries to ensure the modeled configuration is consistent with what you want to update on the device.

Job Manager—This NetScreen-Security Manager module tracks the status of running and completed update processes. The Job Manager displays details of the update process in a dedicated information window and includes the update's success or failure and errors involved in a failed update.

The Update Lifecycle

The lifecycle of the update process:

1. The managed device is functioning normally. You have successfully added the device to NetScreen-Security Manager, reviewed the device configuration, and updated the device. Suddenly, an event occurs on the managed device that requires a change to the device configuration. For example, malicious traffic might have entered your network, causing you to update the Security Policy for the device to detect and prevent that attack.

2. You locate the cause of the event. Using NetScreen-Security Manager modules such as the Realtime Monitor and Log Viewer, you determine the exact attack that penetrated the device. From the Report Manager, you also determine what rule in the Security Policy was ineffective in blocking the attack. You then update the modeled device configuration, editing the Security Policy to detect and prevent the attack from entering your network again.

3. Before updating the running configuration, you review the modeled device configuration. Using a delta configuration summary, compare the modeled configuration with the running configuration on the device to confirm the differences. Fine-tune the modeled configuration, if needed.

4. When you are confident that the modeled configuration is valid, update the device. NetScreen-Security Manager updates the running configuration with only the new changes (delta); During the update, you track the update progress using Job Manager. In the job information window, you can track the progress of the update real-time and observe the transfer of the configuration from NetScreen-Security Manager to the device.

If the update is unsuccessful, use the information in the Job information window to correct the problems in the modeled configuration.

5. After updating, run a second Delta Configuration Summary to identify any remaining differences between the modeled configuration and the running configuration on the device. When the Delta Configuration Summary reveals no differences between the new configuration and the old configuration on the device, you have successfully updated the running configuration.
About Atomic Configuration (ScreenOS 5.x Only)

NetScreen-Security Manager uses atomic configuration, a fail-safe feature for security devices running ScreenOS 5.x. Atomic configuration ensures a current valid configuration is not overwritten by a flawed configuration in flash memory. The update must complete without errors and the device connection to the management system must remain active, or the update is aborted to prevent an invalid, error-prone, or flawed configuration to install on the device.

Atomic configuration is always on. During an update:

1. NetScreen-Security Manager saves and locks the active configuration on the device, then starts a timer for the update process. While the active configuration is locked, it cannot be saved.

2. NetScreen-Security Manager sends the modeled configuration to the device.

3. As the device receives the modeled configuration, it updates its existing active configuration with each command as the command is received:

   - If the device executes the entire modeled configuration (all commands) and the connection to the management system remains up, NetScreen-Security Manager unlocks the active configuration and saves the new active configuration.

   - If the device cannot execute a command, NetScreen-Security Manager resets the device, unlocks the active configuration, and restores the saved active configuration to the device (the device reboots). After rebooting, the device sends a final error message to the management system; this contents of this message, which include any CLI errors in the failed configuration, appear in the Job Manager status window for this update.

   - If the device connection to the management system is down after all commands have been executed, the update timer expires and the device automatically resets. The device unlocks the active configuration and restores the saved active configuration (the device reboots). The connection might be down due to a command in the modeled configuration that causes the device to lose connection with the NetScreen-Security Manager Device Server.

NOTE: When updating vsys devices, atomic configuration occurs only for the root vsys.

About Atomic Updating (ScreenOS 5.1 or Higher Only)

In addition to atomic configuration, devices running ScreenOS 5.1 and higher also support atomic updating, which enables the device to receive the entire modeled configuration (all commands) before executing those commands (instead of executing commands as they are received from the management system). Because NetScreen-Security Manager sends all commands at one time, the performance of the management connection is enhanced.
Atomic updating also enables the device to temporarily lose connection to NetScreen-Security Manager during the update process. If the management connection is down when the device has completed executing the commands in the modeled configuration, the device reestablishes the connection. Because the device no longer needs to maintain a constant connection to the management system during updating, you can configure changes to management connection from the NetScreen-Security Manager UI.

During an atomic update:

1. NetScreen-Security Manager saves and locks the active configuration on the device, then starts a timer for the update process (timeout: two hours). While the active configuration is locked, it cannot be saved.

2. NetScreen-Security Manager sends the modeled configuration to the device.

3. The device receives all commands before executing the commands on its existing active configuration. During the update, the device sends progress messages to the management system every 15 seconds; these messages appear in the Job Manager status window for the update.

During the update, the Job Manager status window displays other messages, depending on the success of the update:

- **Updates Without Errors**—If the device executes the entire modeled configuration (all commands) and the connection to the management system remains up or can be reestablished, NetScreen-Security Manager unlocks the active configuration and saves the new active configuration. The device sends a final message to the management system; this message appears in the Job Manager status window for this update.

- **Updates With Errors**—If the device cannot execute a command, it notifies the management system, which makes a decision whether to ignore and proceed, abort, or revert.
  - For ignore and proceed decisions, the device continues the update.
  - For abort and revert decisions, the device automatically resets. The device unlocks the active configuration and restores the saved active configuration (the device reboots). After rebooting, the device sends a final error message to the management system; this message, which includes any CLI errors in the failed configuration, appears in the Job Manager status window for this update.

- **Re-establish Management Connection**—If the device connection to the management system is down after all commands have been executed, the device attempts to reestablish connectivity.
  - If successful, NetScreen-Security Manager unlocks the active configuration and restores the saved active configuration to the device. The device sends a final message to the management system; this message appears in the Job Manager status window for this update.
If attempts to reconnect are unsuccessful for two hours, the update timer expires and the device automatically resets. The device unlocks the active configuration and restores the saved active configuration (the device reboots). After rebooting and reestablishing connection to the management system, the device sends a final error message to the management system; this message, which includes any CLI errors in the failed configuration, appears in the Job Manager status window for this update.

Retrying a Failed Update

When updating your managed security devices, the update fails for each device that is not connected to the management system at the time of update. For device running ScreenOS 5.1 and higher, you can configure NetScreen-Security Manager to save the pending changes for an unconnected device, then install those changes when the device finally connects to the management system.

NetScreen-Security Manager automatically changes the configuration state of an unconnected device that is waiting for changes to the “Sync Pending” state. When a device in this state connects to the management system, pending changes are immediately installed on the device and the configuration state is changed to “In-Sync”.

You can also configure the management system to abort update attempts for previously unconnected devices to which out-of-band changes have been made. For example, you attempt to update all your managed NS-5GT security devices, but device NS-5GT-25 is disconnected from the management system for troubleshooting at the time of update. When troubleshooting is complete and the device reconnects, to prevent NetScreen-Security Manager from overwriting any out-of-band changes made, enable the option “Don’t Update If Device Has Changed”.

Configuring Update Options

You can configure device update and retry options on a system-wide basis (in the UI preferences), on a per-update basis for multiple devices (in the device update dialog box), and on a per-update basis for a single device (in the device options dialog box). The system-wide settings appear as the default settings for the both per-update settings, which you can change as needed for each update.

When configuring system-wide update options, you can enable or disable any option independently; when configuring per-update options, dependencies apply.

Update options include:

- Rematch, Session Treatment when modifying a policy rule—When enabled, NetScreen-Security Manager preserves the existing sessions that are being tracked by the installed Security Policy during the policy update procedure (devices running ScreenOS 5.1 or higher only). At the end of the update, NetScreen-Security Manager restores all valid sessions on the managed device and deletes all invalid sessions.

  When disabled, NetScreen-Security Manager does not preserve and restore existing sessions for a updated managed device.
Show Unconnected Devices in Device Selection Dialog—When enabled, the NetScreen-Security Manager UI displays devices that are not connected to the management system in the Update Devices dialog box (which displays when you attempt to update the configuration for a managed device).

When disabled, unconnected devices do not appear in the Update Devices dialog box, preventing admins from selecting an unconnected device for updating.

When configuring this option on a per-update basis, you must enable this option before the “Update When Device Connects” option is available.

Update When Device Connects—When enabled, NetScreen-Security Manager attempts to update a previously unconnected device with pending changes stored in the management system.

If you do not select this option, NetScreen-Security Manager attempts to update the device, but fails because the device is unreachable. The failed attempt is listed in the job manager.

When configuring this option on a per-update basis, you must enable this option before the “Don’t Update If Device Has Changed” option is available.

Don’t Update If Device Has Changed—When enabled, NetScreen-Security Manager does not update a previously unconnected device if out-of-band changes have been made to the device. The configuration state of the device remains as “Sync Pending”.

Enable Option Dialog—When enabled, NetScreen-Security Manager displays device update options for single-device updates. The update options dialog box appears when you right-click a device in Device Manager and select Update

Attacks.

When disabled, the update options dialog box does not appear for single-device updates initiated from the Device Manager. Alternatively, to disable from within the per-update device update dialog box, select the option “Don’t Show This Dialog”.

Knowing When to Update

You might need to update a device configuration for one or more reasons. Typically, you update a device after changing the device configuration or after modifying the Security Policy that is assigned to the device.

To overwrite the existing configuration on the physical device, update the physical device with the modeled configuration in NetScreen-Security Manager.

To overwrite the modeled configuration in NetScreen-Security Manager, import the existing configuration from the physical device. Currently, NetScreen-Security Manager does not support delta updates from the device.
Using NetScreen-Security Manager, you can identify the changes made to the device or to the modeled configuration, then update the device. For significant changes to the network that the security device is deployed in, you might also need to change the assigned policy.

Check the following areas to detect configuration or policy changes:

- Verifying Device Status in Device Monitor
- Verifying Device Status in Device Manager
- Reviewing Logs
- Identifying Administrative Changes
- Reviewing Reports

**Verifying Device Status in Device Monitor**

Within the management system, a managed device has an associated connection state and configuration state. NetScreen-Security Manager displays each status for each managed device in RealTime Monitor > Device Monitor.

For more details on using the Device Monitor, see “Monitoring Security Devices” on page 682.

**Connection Status**

The connection state indicates the status of managed device–Device Server connection. NetScreen-Security Manager uses heartbeat packets to continually test the connection between the Device Server and the physical device, and the connection status column in the Device Monitor displays the current status of the device:

- **Up status**—Indicates the device is connected to the Device Server and is running properly. Before you can update a device, it must be in the Up state.

- **Down status**—Indicates that an event has occurred, either manually by an administrator or automatically by the flow of a type of traffic, that has stopped the device from running.

- **Never Connected status**—Indicates that the device has not made an initial connection to Device Server. Typically, this state appears for modeled devices that have not been activated, or for devices waiting to be activated using Rapid Deployment.

**Configuration Status**

The configuration state indicates the status of the device configuration on the physical device. Some common configuration states:

- **Managed**—Indicates that the running configuration is the same as the modeled configuration (the device is using a “managed” configuration).
- Modeled—Indicates that the running configuration is not the same as the modeled configuration, and that the device has not yet connected to NetScreen-Security Manager.

- Import Needed—Indicates that the running configuration is not the same as the modeled configuration, but the device has connected to NetScreen-Security Manager and is awaiting manual import (this configuration status occurs only when adding devices running ScreenOS 5.x to the management system).

- Update Needed—Indicates that the running configuration is not the same as the modeled configuration, and that the device is connected to NetScreen-Security Manager. You must update the managed device before the changes you made in the modeled configuration can take effect.

For devices running ScreenOS 5.1 and higher, NetScreen-Security Manager supports additional configuration states that indicate the status of the physical device configuration in relation to the modeled configuration in NetScreen-Security Manager. In addition to the states listed above, a device running ScreenOS 5.1 and higher can have one of the following four configuration states:

<table>
<thead>
<tr>
<th>Detail State</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managed, In Sync</td>
<td>The physical device configuration is synced with the modeled configuration in NetScreen-Security Manager.</td>
</tr>
<tr>
<td>Managed, Device Changed</td>
<td>The physical device configuration is out-of-sync with the modeled configuration in NetScreen-Security Manager. Changes were made to the physical device configuration (the configuration on the physical device is newer than the modeled configuration). To correctly synchronize the two configurations, import the configuration from the physical device.</td>
</tr>
<tr>
<td>Managed, NSM Changed</td>
<td>The modeled device configuration is out-of-sync with the physical device configuration. Changes were made to the modeled configuration (the configuration on the NetScreen-Security Manager is newer than the physical device configuration). Any change made in the UI automatically causes the NSM configuration state to change, even when the change is canceled or undone. For example, if you change a value in the UI to a different value, then undo the change by entering the original value, the NSM configuration state is still considered out-of-sync with the physical device. To correctly synchronize the two configurations, update the configuration on the physical device.</td>
</tr>
<tr>
<td>Managed, NSM and Device Changed</td>
<td>Both device configurations (physical and modeled) are out-of-sync each other. Changes were made to the physical device configuration and to the modeled configuration. Although you cannot sync delta changes, you can run a delta config summary (see “Using a Delta Configuration Summary” on page 400) to identify the differences, then manually make the changes to the modeled configuration and update the device.</td>
</tr>
<tr>
<td>Managed, Sync Pending</td>
<td></td>
</tr>
</tbody>
</table>

Changing the name, color, or NetScreen-Security Manager port on a device causes the configuration state to be out of sync, even though the management system and device do not share these parameters (these parameters are not transmitted to or from the device during an update).
Verifying Device Status in Device Manager

You can view the connection and configuration status for each managed device in Device Manager.

NetScreen-Security Manager automatically updates the device status and displays the state of each device in the UI. To view device status, simply place your mouse cursor over the device name. A tooltip appears stating the device name, device type and ScreenOS version, IP address, domain, and the connection and configuration states.

To manually verify the configuration status for devices running ScreenOS 5.1 and higher:

- For a single device—Right-click the device and select Check Config Sync Status. This option appears only for devices running ScreenOS 5.1 and higher.
- For multiple devices—From the menu bar, select Devices > Configuration > Check Config Sync Status. Select the devices running ScreenOS 5.1 and higher for which you want to view configuration status, then click OK.

NOTE: You can use the directive Check Config Sync Status from any location in the NetScreen-Security Manager UI. (You do not need to have Device Manager selected.)

Reviewing Logs

The Log Viewer can help you identify event patterns on your network. To clarify the pattern in the Log Viewer, create a custom view using filters that display log entries based on specific criteria. To set a column or cell filter, right-click the column or cell that you want to use as the matching criteria and specify the value.

For example:

- To track all events for a specific time period, create a filter on the timestamp column; when applied, the filter displays only the log entries that meet the specified time period.
- To track all events from a specific source IP address, create a filter on source address column; when applied the filter displays only the log entries that use the specified source address.
- To track all events for a specific category or subcategory of log entries, such as Configuration or Attack log entries, create a filter on the category or subcategory column; when applied the filter displays only the log entries with the specified category or subcategory designation.

For more details on using the Log Viewer, see Chapter 12, “Logging”. For step-by-step instructions on creating a filter, see the NetScreen-Security Manager Online Help topic “Setting Filters”.

For details on all states, see “Viewing Device Status” on page 683.
Identifying Administrative Changes

Use the Audit Log Viewer to identify administrative changes made to your managed devices. Audit log entries also detail the administrator who made the change, the action performed, and the date and time of the change. You can track changes by time of logging, administrator name, action, targets, and devices. If an administrator made a change to a device or an object, you might want to update the affected devices.

For details on using the Audit Log Viewer, see “Using the Audit Log Viewer” on page 764.

Reviewing Reports

Use Report Manager to determine when you are receiving too many attacks of a certain type and order them by an IP address. For example, if you determine that the current device configuration and Security Policy cannot block scans, you might want to create a new rule in the Security Policy that guards against those attacks, then update the device.

Report Manager provides three reports based on three different criteria: time-based reports, event-based reports, and severity-based reports.

- To identify common events, select an event-based report to see the frequency of events in bar graph or pie chart. To see details for a specific event, right-click the event and select View in Log Viewer to display a custom view in a new window. You can save a detailed view as a custom report. For example, when viewing the Top Alarms, expand a location to view the data that makes up this location.

- To examine how specific rules in your Security Policy are performing, select the Administrative > Top Rules report. You might need to fine-tune an inefficient rule to better handle events in your network traffic.

For details on using Report Manager, see Chapter 13, “Reporting”.

Using Preview Tools

When you update a managed device, you are overwriting the existing configuration that is running on the physical device. Although you can use domain versioning to recover from invalid configurations, ideally, you should verify a configuration before sending it to the device.

Using preview tools, you can preview how the modeled configuration looks in CLI command form to predict the success of the update and anticipate errors. NetScreen-Security Manager supports three types of preview tools:

- Configuration Summary—Displays the modeled configuration using ScreenOS CLI commands.

- Delta Configuration Summary—Displays the modeled configuration and running configuration using ScreenOS CLI commands, and lists the differences between the two configurations.
Running Config—Displays the configuration installed on the physical device.

The configuration and delta configuration summaries help you ensure that the modeled configuration is correct before you update your managed devices, while the running config helps you identify settings already on the managed device.

Running a Configuration Summary

When you update a managed device using NetScreen-Security Manager, the management system generates ScreenOS CLI commands that map to the settings in the NetScreen-Security Manager UI. To verify the configuration you are installing on the device generates the correct CLI commands, run a configuration summary.

1. From the file menu, select Devices > Configuration > Summarize Config. NetScreen-Security Manager displays the Get Configuration Summary dialog box.

2. Select the devices or device groups for which you want to run a Configuration Summary and click OK. A Job Information window appears to help you track the progress of the summary.

3. When the job completes, review the CLI commands in the Job Information window. When you update the device, these are the commands that NetScreen-Security Manager uses to overwrite the running configuration.

For some settings, the CLI commands for a UI settings do not map one-to-one. For example, a single vsys configuration in the NetScreen-Security Manager UI generates multiple ScreenOS commands.

Because the management system generates all information (UI settings and CLI commands) for a configuration summary, you can run a configuration summary on a modeled device (the device does not need to physically exist).

Using a Delta Configuration Summary

A Delta Configuration Summary compares the active configuration on the device with the modeled configuration in NetScreen-Security Manager and displays the differences between the two configurations. The Delta Configuration Summary produces four sets of data.

Table 17: Delta Configuration Summary Information

<table>
<thead>
<tr>
<th>Delta Config Data</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config on Device but not on NSM</td>
<td>Displays the CLI commands detected on the device that do not map to NetScreen-Security Manager settings. Use this information to identify any out-of-band updates (made by the local device admin) to the running configuration; you might not want to overwrite these settings.</td>
</tr>
<tr>
<td>Config on NSM but not on Device</td>
<td>Displays the CLI commands (as mapped to NetScreen-Security Manager settings in the modeled configuration) detected in NetScreen-Security Manager but not on the device. Use this information to identify the changes you have made to the modeled configuration since the last update.</td>
</tr>
</tbody>
</table>
Chapter 6: Updating Devices

You should run a Delta Configuration Summary two times:

- **Before updating**—Because you are overwriting the running configuration with the modeled configuration, you might want to identify and verify the configuration you are installing on the device.

- **After updating**—Ensure that the device received the configuration as you expected, and that no differences exist between the running configuration and the modeled configuration.

Delta configuration summaries are helpful tools for ongoing device maintenance too, particularly for devices that are managed locally by a device administrator using CLI commands or the WebUI and remotely by a NetScreen-Security Manager administrator using the NetScreen-Security Manager UI. Because the modeled configuration can overwrite the running configuration, you should always confirm the commands that are sent to the device.

To run a Delta Configuration Summary:

1. From the file menu, select Devices > Configuration > Summarize Delta Config. NetScreen-Security Manager displays the Get Delta Config Summary dialog box.

2. Select the devices or device groups for which you want to run a Delta Config Summary and click OK. A Job Information window appears to help you track the progress of the summary.

3. When the job completes, review the CLI commands in the Job Information window. Specifically, review the commands in the section “Config to be sent to device on next Update Device”; when you update the device, these are the commands that NetScreen-Security Manager uses to overwrite the running configuration.

An example Delta Configuration Summary is shown below:

<table>
<thead>
<tr>
<th>Delta Config Data</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config on both NSM and Device but reordered</td>
<td>Displays the CLI commands for configuration settings present on both the device and NetScreen-Security Manager, but the CLI command sequence has been reordered.</td>
</tr>
<tr>
<td>Config to be sent to device on next Update Device</td>
<td>Displays the CLI commands that NetScreen-Security Manager will send to the device on the next update.</td>
</tr>
</tbody>
</table>
### Figure 94: Delta Configuration Summary Example

<table>
<thead>
<tr>
<th>Config on Device but not on NSM:</th>
<th>Commands for objects already configured on the device</th>
</tr>
</thead>
<tbody>
<tr>
<td>unset interface serial manage telnet</td>
<td>set zone untrust screen syn-flood</td>
</tr>
<tr>
<td>unset interface serial manage web</td>
<td>set zone untrust screen syn-flood alarm-threshold 512</td>
</tr>
<tr>
<td>unset interface serial manage ssl</td>
<td>set zone untrust screen syn-flood attack-threshold 200</td>
</tr>
<tr>
<td>unset interface serial manage snmp</td>
<td>set zone untrust screen syn-flood queue-size 1024</td>
</tr>
<tr>
<td>unset interface serial manage scs</td>
<td>set zone untrust screen syn-flood timeout 20</td>
</tr>
<tr>
<td>unset interface serial manage ping</td>
<td>set zone untrust screen syn-flood source-threshold 512</td>
</tr>
<tr>
<td>unset av http trickling</td>
<td>set zone untrust screen syn-flood destination-threshold 1024</td>
</tr>
<tr>
<td>set av all max-connections 0</td>
<td>set policy id 1 from trust to untrust Any Any ANY permit</td>
</tr>
<tr>
<td>set zone untrust screen syn-flood</td>
<td>set nsrp ha-link probe threshold 5</td>
</tr>
<tr>
<td>set zone untrust screen syn-flood alarm-threshold 512</td>
<td>set nsrp ha-link probe interval 1</td>
</tr>
<tr>
<td>set zone untrust screen syn-flood attack-threshold 200</td>
<td>set nsrp vsd-group init-hold 5</td>
</tr>
<tr>
<td>set zone untrust screen syn-flood queue-size 1000</td>
<td></td>
</tr>
<tr>
<td>set zone untrust screen syn-flood timeout 20</td>
<td></td>
</tr>
<tr>
<td>set zone untrust screen syn-flood source-threshold 512</td>
<td></td>
</tr>
<tr>
<td>set zone untrust screen syn-flood destination-threshold 1000</td>
<td></td>
</tr>
<tr>
<td>set policy id 700029 from trust to untrust Any Any ANY permit</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Config on NSM but not on Device:</th>
<th>Commands for Objects configured in NetScreen-Security Manager.</th>
</tr>
</thead>
<tbody>
<tr>
<td>set pppoe name untrust</td>
<td></td>
</tr>
<tr>
<td>set zone untrust screen syn-flood</td>
<td></td>
</tr>
<tr>
<td>set zone untrust screen syn-flood alarm-threshold 512</td>
<td></td>
</tr>
<tr>
<td>set zone untrust screen syn-flood attack-threshold 200</td>
<td></td>
</tr>
<tr>
<td>set zone untrust screen syn-flood queue-size 1000</td>
<td></td>
</tr>
<tr>
<td>set zone untrust screen syn-flood timeout 20</td>
<td></td>
</tr>
<tr>
<td>set zone untrust screen syn-flood source-threshold 512</td>
<td></td>
</tr>
<tr>
<td>set zone untrust screen syn-flood destination-threshold 1000</td>
<td></td>
</tr>
<tr>
<td>set policy id 700029 from trust to untrust Any Any ANY permit</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Config on both Device and NSM but reordered:</th>
<th>Commands on the device and NetScreen-Security Manager that have been reordered.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Occasionally, the delta configuration report might display discrepancies that do not actually exist between the running configuration and the modeled configuration. In some specific situations, the running configuration includes CLI commands that do not appear as pending changes in NetScreen-Security Manager, yet the two configurations are actually in sync (no deltas exist). This can occur when:

- Some settings for a feature have been configured in NetScreen-Security Manager, but the feature itself is not enabled. For example, if you configure NSRP settings but do not deploy the device in NSRP mode, the CLI commands for NSRP settings appear in the running configuration but are not managed by NetScreen-Security Manager (because the feature is not active).

- DHCP settings, such as interface IP addresses, are not assigned by NetScreen-Security Manager, and are not included in the CLI commands sent to the device. The CLI commands do appear, however, in the running configuration.

- Default, unconfigured settings might not be managed NetScreen-Security Manager. For example, if the running configuration includes the domain name mycompany.net, but that domain name is not configured in NetScreen-Security Manager, the management system leaves the value unchanged.

Performing an Update

You can update a single device, multiple devices, or device groups using the same process.

Before updating:

- Ensure that you have configured the device correctly, created and assigned a policy to the device, and have established a connection between the device and the management server.
Performing an Update

Run a Configuration Summary on the device to view the CLI commands for the modeled configuration. Review these commands to ensure that you have configured the device as desired.

Run a Delta Configuration Summary to view the differences between the modeled configuration and the running configuration in CLI command format.

Update the device:

1. From the menu bar, select Devices > Configuration > Update Config. NetScreen-Security Manager displays the Update Devices dialog box.

2. Select the devices or device groups you want to update and click OK. NetScreen-Security Manager begins updating the selected devices or device groups with the modeled configuration.

After updating:

- Review the information in the Job Information window to determine if the update was successful.
- NetScreen-Security Manager automatically runs a Delta Configuration Summary after a successful update. Review the summary to ensure that no conflict exist between the running configuration and the modeled configuration.

retrying a failed update

When updating your managed security devices, the update fails for each device that is not connected to the management system at the time of update. For device running ScreenOS 5.1 or higher, you can configure NetScreen-Security Manager to save the pending changes for an unconnected device, then install those changes when the device finally connects to the management system.

NetScreen-Security Manager automatically changes the configuration state of an unconnected device that is waiting for changes to the “Sync Pending” state. When a device in this state connects to the management system, pending changes are immediately installed on the device and the configuration state is changed to “In-Sync”.

You can also configure the management system to abort update attempts for previously unconnected devices to which out-of-band changes have been made. For example, you attempt to update all your managed NS-5GT security devices, but device NS-5GT-25 is disconnected from the management system for troubleshooting at the time of update. When troubleshooting is complete and the device reconnects, to prevent NetScreen-Security Manager from overwriting any out-of-band changes made, enable the option “Don’t Update If Device Has Changed”.

Configuring Update Options

You can configure device update and retry options on a system-wide basis (in the UI preferences), on a per-update basis for multiple devices (in the device update dialog box), and on a per-update basis for a single device (in the device options dialog box). The system-wide settings appear as the default settings for the both per-update settings, which you can change as needed for each update.
When configuring system-wide update options, you can enable or disable any option independently; when configuring per-update options, dependencies apply.

Update options include:

- **Rematch, Session Treatment when modifying a policy rule**—When enabled, NetScreen-Security Manager preserves the existing sessions that are being tracked by the installed Security Policy during the policy update procedure (devices running ScreenOS 5.1 or higher only). At the end of the update, NetScreen-Security Manager restores all valid sessions on the managed device and deletes all invalid sessions.

  When disabled, NetScreen-Security Manager does not preserve and restore existing sessions for a updated managed device.

- **Show Unconnected Devices in Device Selection Dialog**—When enabled, the NetScreen-Security Manager UI displays devices that are not connected to the management system in the Update Devices dialog box (which displays when you attempt to update the configuration for a managed device).

  When disabled, unconnected devices do not appear in the Update Devices dialog box, preventing admins from selecting an unconnected device for updating.

  When configuring this option on a per-update basis, you must enable this option before the “Update When Device Connects” option is available.

- **Update When Device Connects**—When enabled, NetScreen-Security Manager attempts to update a previously unconnected device with pending changes stored in the management system.

  When disabled, NetScreen-Security Manager does not update a previously unconnected device, and the configuration state of the device remains as “Sync Pending”.

  When configuring this option on a per-update basis, you must enable this option before the “Don’t Update If Device Has Changed” option is available.

- **Don’t Update If Device Has Changed**—When enabled, NetScreen-Security Manager does not update a previously unconnected device if out-of-band changes have been made to the device. The configuration state of the device remains as “Sync Pending”.

- **Enable Option Dialog**—When enabled, NetScreen-Security Manager displays device update options for single-device updates. The update options dialog box appears when you right-click a device in Device Manager and select Update Attacks.

  When disabled, the update options dialog box does not appear for single-device updates initiated from the Device Manager. Alternatively, to disable from within the per-update device update dialog box, select the option “Don’t Show This Dialog”.

Performing an Update  ■  405
Tracking Device Updates

Use Job Manager to track device updates in real-time. You can view the status of a running update and the status of completed updates in the Job Manager module.

When you send a command to a device or group of devices using NetScreen-Security Manager, the management system creates a job for that command and displays information about that job in the Job Information window. The command you send the device is called a directive; Job Manager tracks the progress of the directive as it travels to the device and back to the management system. Each job contains:

- Name of the command
- Date and time the command was sent
- Completion status for each device that received the command
- Detailed description of command progress
- Command output, such as a configuration list or CLI changes on the device

NOTE: Job Manager configuration summaries and job information details do not display passwords in the list of CLI commands for administrators that do not have the assigned activity “View Device Passwords”. By default, only the super administrator has this assigned activity.

You can initiate directives from multiple locations in the NetScreen-Security Manager UI, including the Devices and Tools menus in the NetScreen-Security Manager toolbar (to access the Update directive, from the file menu, select Devices > Configuration > Update Device Configuration). The Job Manager module is shown below:
Job Manager includes the following utilities and information:

- **View Controls**—Use View controls to set the information level you want displayed in Job Manager:
  - Expand All displays all devices associated with a directive type.
  - Collapse All displays the directive type.

- **Job Type (Directive) List**—Displays the job type (directives) and associated timestamp completion status information. All current and completed jobs appear, including device updates. However, if you have not yet performed an update using NetScreen-Security Manager, the Job List does not display an Update Configuration directive.

- **Notification Controls**—Enables you to manually view job completion status.

- **Job Information**—Enables you to view various types of job information including errors, job completion status, job state, automatic job completion notification setting, and start time of job.

### Reviewing Job Information

The Job Information dialog box displays the changing device states as the directive is executed. Device state changes, error messages, and warning messages are displayed in real-time. An example Job Information dialog box is shown below:

```
<table>
<thead>
<tr>
<th>Name</th>
<th>Timestamp</th>
<th>Completion</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config Summary</td>
<td>Tue Dec 16 14:53:3...</td>
<td>2 of 2</td>
<td>Successful Completion</td>
</tr>
<tr>
<td>Import Config</td>
<td>Tue Dec 16 14:53:3...</td>
<td>1 of 1</td>
<td>Successful Completion</td>
</tr>
<tr>
<td>Reboot Device</td>
<td>Tue Dec 16 14:53:3...</td>
<td>1 of 1</td>
<td>Successful Completion</td>
</tr>
<tr>
<td>Update Device</td>
<td>Tue Dec 16 14:53:3...</td>
<td>1 of 1</td>
<td>Successful Completion</td>
</tr>
<tr>
<td>Delta Config Summary</td>
<td>Tue Dec 16 14:53:3...</td>
<td>1 of 1</td>
<td>Successful Completion</td>
</tr>
</tbody>
</table>
```
Job Manager tracks the overall progress of one or more jobs executed on a single device. For multiple device updates, Job Manager tracks the progress of each job on each device in addition to the overall progress for all devices. To view the Job status for an individual device (including error messages and percent complete), select the device in the Percent Complete pane; the status appears in the Output pane.

The Job Information includes:

- **Job Type**—The type of task being tracked. Job Types include Update Device, Reboot Device, and Config Summary. Job Type is also known as a directive.
- **Time Stamp**—The time that NetScreen-Security Manager began executing the directive.
- **Job Status**—The current state of the job.
- **Number of Jobs Completed**—The number of jobs completed out of the total number of jobs.
- **Percent Complete**—The percentage of total jobs successfully executed. When performing multiple jobs on multiple devices, this number displays the percentage complete for each device. When the job has completed, successfully or unsuccessfully, the percent complete displays 100 percent.
- **Device Name**—The name of the device on which the job is executed.
- **State Description**—The current state of the job.
- **Completion Level**—The percentage of the total job that has executed successfully.
Output—Displays content of the update, including commands that have been interpreted from the NetScreen-Security Manager data model into ScreenOS commands, error messages, and existing commands deleted from the device. The Output Display Region displays all errors, warnings, device verification output, and device state information associated with the job.

NOTE: Job Manager configuration summaries and job information details do not display passwords in the list of CLI commands for administrators that do not have the assigned activity “View Device Passwords”. By default, only the super administrator has this assigned activity.

Device States During Update

During an update, the managed device changes device state. You can view the current device state in real-time in the State Description field of the Job Information dialog box. A device can have the following states:

Table 18: Device States During Update

<table>
<thead>
<tr>
<th>Device State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>No update activity has occurred on the device.</td>
</tr>
<tr>
<td>Loading in Progress</td>
<td>NetScreen-Security Manager is sending the update image into the Flash memory of the device.</td>
</tr>
<tr>
<td>Pending</td>
<td>Device is accepting the parameters from the update configuration that has been sent to the device Flash memory.</td>
</tr>
<tr>
<td>Converting Data Model to Device Data Model</td>
<td>The parameters that have been set in the NetScreen-Security Manager configuration are being changed to corresponding ScreenOS CLI commands that execute on the device.</td>
</tr>
<tr>
<td>Completion</td>
<td>Device has successfully been updated with the modeled configuration.</td>
</tr>
<tr>
<td>Failed</td>
<td>Device has not been successfully updated with the modeled configuration. The Output pane of the Job Manager dialog box displays error messages and error codes.</td>
</tr>
</tbody>
</table>

The update process for devices running ScreenOS 4.0.x or ScreenOS 5.x is identical.

Understanding Updating Errors

When an update fails for any reason, Job Manager displays error codes and error messages that can help you identify and locate the problem. Typical errors include:

- The modeled configuration contained invalid values that the device could not process.
- During the update process, the connection between the managed device and the Device Server was lost.
- The modeled configuration caused the managed device to lose its connection to NetScreen-Security Manager. For these update errors, the Job Information dialog box displays the Job Status as “Failed.”
You can also check the Connection Status and Configuration Status columns for the device in the Realtime Monitor to determine if the device is running.

After a device is updated, NetScreen-Security Manager automatically runs a Delta Configuration Summary to determine any remaining differences between the modeled configuration and the running configuration; the output of this summary appears in the Job Manager information window. For successful updates, no discrepancies are found or displayed. For failed updates, the output area lists remaining discrepancies.

For example, a failed update job is shown below:

Figure 98: Failed Update Job Dialog Box

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Error Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inactivated Command</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Operation Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commands Deleted from Device</td>
</tr>
</tbody>
</table>

| New Commands updated on the Device |

In the Output area of this job, the update:

- Successfully removed existing commands on the device (Generating Removing CLI Commands)

- Unsuccessfully added new commands that were not present in the running configuration (Generated 5 Delta Config CLI Commands). Specifically, the update could not set the command: `pppoe name untrust clear-on-disconnect`

The Delta Config Summary correctly detected a difference between settings on the managed device and settings in NetScreen-Security Manager. This error might be the result of a disabled command, possibly disabled by another NetScreen-Security Manager administrator or a local device administrator.
Chapter 7
Managing Devices

This chapter describes device management tasks you might need to perform in specific situations, such as upgrading the ScreenOS version on your devices, obtaining and activating a Deep Inspection subscription, and handling an RMA device in the NetScreen-Security Manager UI.

This chapter also provides details on how the components of the NetScreen-Security Manager management system handle device capabilities, and how device configuration settings are imported and updated. This material is provided for reference only, and does not contain specific configuration tasks.

The following sections are in this chapter:

- Managing Device Firmware Version
- Managing License Keys
- Activating Subscription Services
- Managing the Attack Database
- Updating AV Pattern Files
- Updating the URL Category List
- Miscellaneous Device Operations
- Managing Device Capabilities
- Archiving and Restoring
Managing Device Firmware Version

You can use Juniper Networks NetScreen-Security Manager to upgrade or adjust the firmware on a device running ScreenOS 4.0.x or 5.x.

**NOTE:** NetScreen-Security Manager does not support the upgrade of NetScreen-500 and ISG 2000 security devices from ScreenOS 5.1 to ScreenOS 5.2. This migration requires a bootrom upgrade; for more details, refer to the ScreenOS 5.2 Migration Guide.

Upgrading Device Firmware Version

To upgrade the firmware, first download the new firmware image file to your computer. Next, use the Firmware Manager in NetScreen-Security Manager to copy the image file to the GUI Server, where it is permanently stored, then select the devices and the firmware image files you want to use to upgrade the device. During the upgrade, the GUI Server copies the image file to the Device Server, where the image file is stored temporarily until the upgrade is complete. After the firmware has been successfully installed, the device automatically reboots.

**NOTE:** Do not change the name of the image file. The name of the image file must be exactly the same as the filename that you download from Juniper Networks, for example, ns5xp.4.0.3r2.0.

When upgrading multiple device types, ensure that you have loaded the same ScreenOS version of the image file for each type of device on the Device Server. For example, you can upgrade the firmware on a NetScreen-208, a NetScreen-50, and a NetScreen-5XP at the same time, but the image files for each device type must exist on the Device Server and must be the same ScreenOS version.

When upgrading firmware on your managed devices, you can use different methods depending on the version of ScreenOS that exists on the devices:

- For devices currently running ScreenOS 4.0.x, you must install a TFTP server on the NetScreen-Security Manager Device Server. The Device Server automatically uses TFTP to load the firmware onto your managed devices. For more information, see the NetScreen-Security Manager Installer’s Guide.

- For devices running ScreenOS 5.x, the Device Server automatically uses Secure Server Protocol (SSP) to load firmware onto your managed devices. SSP is the protocol used for the management connection between the physical device and the NetScreen-Security Manager Device Server.
Select the Automate ADM Transformation option to automatically update the Abstract Data Model (ADM) when the firmware is loaded onto the managed device. If you deselect this option, the firmware is loaded onto the device, but you cannot manage the device from the UI until the ADM is updated. For example, you might want to deselect this option to first verify that the device is properly operating with the uploaded firmware before managing it from the NetScreen-Security Manager UI. To enable management, you must reconcile the firmware that you uploaded on the device with the ADM, as described in “Adjusting Device Firmware Version” on page 413. For more information about the ADM and NetScreen-Security Manager components, see “Managing Device Capabilities” on page 431.

For step-by-step instructions on upgrading a device, see the NetScreen-Security Manager Online Help topic, “Upgrading Firmware on Devices.”

Adjusting Device Firmware Version

When importing or updating devices, NetScreen-Security Manager alerts you if it detects a mismatch between the firmware running on the managed device and the firmware that NetScreen-Security Manager has recorded for the device.

Firmware mismatches can occur when:

- A device administrator changes the firmware on the device using the WebUI or CLI commands (through a console, Telnet, or SSH session).

- The Automate ADM Transformation option in the Firmware Update Availability dialog box was deselected during a firmware upgrade by NetScreen-Security Manager. (See “Upgrading Device Firmware Version” on page 412.)

To reconcile the firmware versions, right-click a device and select Adjust OS Version to display the Adjust OS Version Wizard. Follow the directions in the wizard. For step-by-step instructions on upgrade a device, see the NetScreen-Security Manager Online Help topic, “Adjusting the Firmware Version on Devices.”

Downgrading Device Firmware Version

NetScreen-Security Manager does not support firmware downgrades; you cannot use NetScreen-Security Manager to install an earlier version of Juniper Networks ScreenOS firmware than is currently running on the device. You must use the WebUI or ScreenOS CLI commands to downgrade a managed device, then re-add the device to NetScreen-Security Manager.

Upgrading Device Support

Use the Upgrade Device Support directive to automatically upgrade all existing devices that are eligible to provide forward or full management support for features in a future release of ScreenOS.

NOTE: You must install a schema patch for the future version of ScreenOS before upgrading the device support.

The directive performs the following actions:
Managing License Keys

Some security devices support the activation of optional features or the increased capacity of existing features through the installation of license keys. You must first obtain a license key from your value-added reseller (VAR) or from Juniper Networks, then you can use the NetScreen-Security Manager UI to install the license key on the managed device.

After you have installed the license key on the device, the device can begin to use the new feature immediately. However, because the information in the license key is decoded only after it has been installed on the device, you must import the license key information from the device into the NetScreen-Security Manager system before the new feature displays in the UI. Importing license keys from the device can also resolve any license key mismatches between NetScreen-Security Manager and the managed device.

Installing License Keys

The procedure for obtaining a license key is as follows:

1. Contact the value-added reseller (VAR) who sold you the security device, or contact Juniper Networks directly.

2. Provide the serial number of your device and state the feature option you want. The license key is generated and then sent to you via email.

To install the license key on a device using the NetScreen-Security Manager UI:

1. In the main navigation tree, right-click the device on which you want to install the license key and select Admin > Install License Key. The Install License Key dialog box appears.

2. Either copy and paste the license key into the dialog box, or click the Browse button to locate the license key file on your computer.

3. Click OK.

Importing License Key Information

After you install a new license key on a device, either through the NetScreen-Security Manager UI or locally (through the WebUI or CLI) you must import that license key information into the NetScreen-Security Manager system.

Importing license key information from a device also enables you to quickly view all license keys installed on a device, and the features and capacities available on the device.

To import or view license key information:
1. In the main navigation tree, right-click the device on which you want to install the licence key and select Admin > Get License Key Info.

2. Click Yes at the confirmation dialog box. The Job Information window displays the license key information.

**Installing Trial License Keys**

For devices running ScreenOS 5.3 and above, you can install a trial license key. A trial license key allows you to view and evaluate specific features on the device before purchasing the subscription.

**Activating Subscription Services**

To use some Juniper Networks services, such as internal AV or Deep Inspection Signature Service, you must activate the service on the device by first registering the device, then obtaining the subscription for the service. Even though devices with bundled AV services come with a temporary, pre-installed subscription, you must register your product and retrieve the subscription to receive your full paid subscription.

To register your product, go to www.juniper.net/support. After you have registered your product, you can retrieve the service subscription as described in the following section.

To obtain the subscription for a service:

1. From the menu bar, select Devices > Entitlement > Get Entitlement. The Get Entitlement dialog box appears.

2. Select the device(s) or group of devices for which you want to retrieve a subscription.

3. Click OK. The Job Information window displays the status of the subscription retrieval.

**Managing the Attack Database**

The attack object database stored on the device contains predefined attack objects and groups designed to detect known attack patterns and protocol anomalies within network traffic. You use attack object when using Deep Inspection (DI) or Intrusion Detection and Prevention (IDP) as attack detection mechanisms in a Security Policy rule.

To manage the attack database:

- Updating the Attack Object Database—Juniper Networks provides frequent attack database updates, available for download from the Juniper Networks website. New attacks are discovered daily, so it’s important to keep your attack object database up-to-date.

- Verifying the Attack Database Version—The attack database version on the security device and on the NetScreen-Security Manager GUI Server must match.
Updating the IDP Detector Engine—The IDP engine is dynamically changeable firmware that runs on the ISG 2000 or ISG 1000 security device running ScreenOS 5.0.0-IDP1.

Scheduling Security Updates—Configure the NetScreen-Security Manager system to automatically update your security devices with the latest attack objects.

The following sections detail each activity.

Updating the Attack Object Database

You can update the attack object database for managed devices that have Deep Inspection and IDP capabilities. The attack object update occurs differently for devices running different versions of ScreenOS:

- For devices running ScreenOS version 5.0.0-IDP1 or ScreenOS 5.1 and higher, you must download new attack objects from the attack object database server to the GUI Server, then download the new objects to your managed devices.

- For devices running ScreenOS versions 5.0 or earlier, you must configure the devices to contact the attack object database server, then prompt the devices to download new attack objects from the server.

To update a managed device with new attack objects, you must first obtain a DI or IDP subscription for your security device. For details, see “Activating Subscription Services” on page 415.

Updating Attacks on ScreenOS 5.0.0-IDP1, 5.1, and 5.2

You can update attacks for ScreenOS 5.0.0-IDP1, 5.1, and 5.2 devices by downloading new attack objects from the attack object database server to the GUI Server, then downloading the new objects to your managed devices.

You can perform a network update if the NetScreen-Security Manager GUI Server has an Internet connection. During a network update, the GUI Server contacts the Attack Object Database server (managed by Juniper Networks) and automatically downloads the necessary attack object files.

You can perform a local update if the GUI Server does not have Internet connectivity or you do not want to perform a network update. To prepare for a local update, you manually download the attack objects files from the Attack Object Database server (managed by Juniper Networks), then copy these files to a local directory on the GUI Server. Then, during the local update, you specify the path to these files.

Preparing for a Local Update

To perform a local update, you must complete the following steps before attempting the update:

1. Obtain the two attack update files (the data file and the attack object database file) from Juniper Networks website:
For the .dat (data) file, browse to:
https://services.netscreen.com/restricted/sigupdates/nsmfp3-DI-IDP/NSMFP3-DI-IDPAttackUpdateInfo.dat. Copy and paste the content from the URL into a file. NSMFP3-DI-IDPAttackUpdateInfo.dat

For the .zip file (the attack object database), browse to:

2. Save both files to a local directory on the NetScreen-Security Manager GUI Server:

   - Save the .dat file as NSMFP3-DI-IDPAttackUpdateInfo.dat
   - Save the .zip file as NSMFP3-DI-IDP.zip

   DO NOT change the file name. Example of local directory: /tmp/

3. Change the permissions on both files to make them readable by all users.

**Running the Attack Object Update (Local and Network)**

To update the attack object database on the NetScreen-Security Manager GUI Server:

1. From the Tools menu bar, select Preferences. The New Preferences dialog box appears. In the preference navigation tree, select Attack Object.

2. In the Download URL box, configure the URL for the attack update file. When you update the attack object database, the management system contacts this server and downloads the latest database version to the GUI Server.

   - To perform a network update, enter the URL of the Attack Object Database server in the Download URL box. To restore the default server (https://services.netscreen.com/restricted/sigupdates/nsmfp3-DI-IDP/NSMFP3-DI-IDPAttackUpdateInfo.dat), select Restore Defaults.

   - To perform a local update, specify the directory path to the .dat file you previously downloaded in the Download URL box. Example:

     file:///tmp/NSMFP3-DI-IDPAttackUpdateInfo.dat

3. From the menu bar, select Tools > Update NSM Attack Database. The Update NSM Attack Database dialog box appears.

4. Follow the instructions in the Attack Update Manager to download the new Signature and Protocol Anomaly Attack Objects to the NetScreen-Security Manager GUI Server.

After you have updated the attack object database on the GUI Server, you can use that database to update the attack object database on your managed devices.

To download the attack object database update to your managed devices:

1. From the menu bar, select Devices > Deep Inspection > Update Device Attack Database. The Update Device Attack Database dialog box appears.
2. Click Next, then select the managed devices on which you want to install the attack object update.

3. Follow the directions in the Change Device Sigpack wizard to update the attack object database on the selected managed devices.

Updating Attacks on ScreenOS 4.0.x and 5.0 Devices
You can update attacks for ScreenOS 4.0.x and 5.0 devices (not 5.0.0 IDP1) by configuring your managed devices to contact the attack object database server, then prompting the devices to download new attack objects from the server.

To configure the device to contact the attack object database server:

1. In the main navigation tree, select Device Manager > Security Devices, then double-click the device for which you want to configure the database.

2. In the device navigation tree, select Security > AttackDB > Settings.

3. For Attack Database Server, enter https://services.netscreen.com/restricted/sigupdates

4. For Mode, select Update.

5. Click OK to save your changes

For details, see “Configuring the Attack Database” on page 327.

To prompt your managed devices to contact the server for updates:

1. From the menu bar, select Devices > Deep Inspection > Update Device Attack Database. The Update Device Attack Database dialog box appears.

2. Click Next, then select the managed devices that you want to update their attack object database.

3. Follow the directions in the Change Device Sigpack wizard prompt the selected managed devices to update their attack object database.

Using Updated Attack Objects
After you download updated attack objects and groups to the GUI Server (or to the device), any new attack objects in the update are available for selection in NetScreen-Security Manager Object Manager. Additionally, updated IDP attack objects also appear available for selection within an IDP rulebase in a Security Policy.

You can use new and updated DI attack objects immediately within a DI profile (in a firewall rule), or use the new and updated IDP attack object within an IDP rulebase. When you install the Security Policy on your managed security devices:

- For a Security Policy that uses IDP attack objects, NetScreen-Security Manager pushes only the attack objects that are used in IDP rules for the device from the GUI Server to the device.
For a Security Policy that uses DI attack objects, NetScreen-Security Manager pushes all updated signatures from the GUI Server to the device.

**Verifying the Attack Database Version**

New attack objects are added to the attack object database server frequently; downloading these updates and installing them on your managed devices regularly ensures that your network is effectively protected against the latest threats. As new attack objects are added to the attack object database server, the version number of the database increments by 1. When you download a version of the attack object database from the server, NetScreen-Security Manager stores the version number of that database.

**Automatic Verification**

For devices running ScreenOS 5.0.0-IDP1 or 5.1 and higher, the management system uses this database version number to detect and notify you when the stored attack object database on the GUI server is:

- Older than the most recent database available from the attack object database server, and/or
- Newer than the attack object database currently installed on your ScreenOS 5.1 and higher managed devices.

When NetScreen-Security Manager detects that managed device contains an older attack object database version than the one stored on the GUI Server, the UI automatically displays a warning for that device indicating that you should update the attack object database on the device.

**Manual Verification**

You can also manually check to see if the attack object database on the server is more recent than the one on the security device.

To manually check the attack object database version:

2. Select the device(s) or group of devices to be checked.
3. Click OK. The Job Information window displays the status of the version check.
Managing Different Attack Database Versions

Each managed device can contain a different attack object database version, however, the NetScreen-Security Manager GUI Server can contain only one version of the attack object database at one time. Therefore, when you update the device configuration on a device, you must also update the database on the managed device to match the version of the database on the GUI Server (if the version on the GUI Server is more recent). If the version on the managed device is identical to or more recent than the version on the GUI Server, the device ignores the attack object updates.

NOTE: Although each managed device can contain a different attack object database version, we recommend that you use the most recent version of the attack object database available to ensure that your network is protected against the latest threats.

Although devices running 4.0.x or 5.0 update their attack object database independently of the GUI Server, they also must remain in sync with the attack object database version on the management system if you intend to disable attacks at the device level:

- When the databases are in sync, you can disable attacks at the device level.
- When the databases are out of sync, you cannot disable attacks at the device level. You must update the attack object database on the device using the procedure detailed in “Updating Attacks on ScreenOS 4.0.x and 5.0 Devices” on page 418.

For details on disabling attacks, see “Configuring the Attack Database” on page 327.

EXAMPLE: UPDATING DEVICES WITH DIFFERENT ATTACK OBJECT DATABASE VERSIONS

On Monday, you update the attack object database to version 2.0 on the GUI Server, then update two managed devices running ScreenOS 5.2, Device A and Device B. Both devices (and the GUI Server) have the same version of the attack object database.

On Wednesday, in response to a security alert, you update the attack object database to version 2.1 on the GUI server, but install the update on only one of your managed devices, Device A. Device A (and the GUI Server) is now running a different version of the attack object database than Device B.

On Friday, you make miscellaneous configuration changes to Device A and B, then attempt to update both devices with the modeled configuration. During the update, the UI warns you that Device B is running an older version of the attack object database than the GUI Server contains.

Updating the IDP Detector Engine

The IDP engine is dynamically changeable firmware that runs on the ISG 2000 or ISG 1000 security device running ScreenOS 5.0.0-IDP1. Automatic updates to the IDP engine occur when you:
Upgrade security device Firmware—When you upgrade the firmware on an ISG 2000 or ISG 1000 device running ScreenOS 5.0.0-IDP1, the upgraded firmware includes the most recent version of the IDP engine as well as a new version of ScreenOS.

Update Attack Database From GUI Server—When you update attack objects on the security device using the GUI Server, you also automatically update the IDP engine on the device. Because attack database updates are available more often than firmware releases, an attack database update may include a more recent version of the IDP engine than is available on the latest firmware release. For example, an attack database update may contain updated IDP attack objects that can only be used with an updated version of the IDP engine.

You can also manually update the IDP Detector Engine. However, the IDP engine version you install on a ISG 2000 or ISG 1000 device must be compatible with the version of the firmware that is running in the device.

NOTE: You cannot downgrade the IDP engine version on the device.

To update the IDP Engine manually:

1. From the menu bar, select Devices > IDP Detector Engine > IDP Detector Engine. The Change Device Sigpack dialog box appears.

2. Click Next, then select the managed devices on which you want to install the IDP engine update.

3. Follow the instructions in the Change Device Manager to update the IDP engine on the selected device.

NOTE: Updating the IDP engine on a device does not require a reboot of the device.

EXAMPLE: CONFIRM IDP ENGINE VERSION
To see the version of the IDP engine that is currently running on a ISG 2000 or ISG 1000 device:


2. Click Next. The Attack Update Summary displays information about the current version downloaded on the GUI Server and the latest version available from Juniper Networks.
Figure 99: Attack Update Summary

3. Click Cancel to exit the Attack Update Manager.

**Scheduling Security Updates**

For security devices running ScreenOS 5.0.0-IDP1 and 5.1 or higher, you can configure the NetScreen-Security Manager system to automatically update the attack object database on the GUI Server and on those security devices.

**NOTE:** For devices running ScreenOS 5.0.x and lower (except for ScreenOS 5.0.0-IDP1), NetScreen-Security Manager does not automatically install new attack objects on the device but instead flags the device for manual updating using the UI.

Using the command line utility guiSvrCli.sh, you direct the management system to obtain the latest attack objects from the attack database server (managed by Juniper Networks), then specify the action you want the server to take:

- The **none** action option directs the server to update the attack object database on the GUI Server only (the server does not update security devices).
The `update-attack` action option directs the server to update your managed security devices that use Deep Inspection (DI) or Intrusion Detection and Prevention (IDP).

For a successful update, the device configuration must be "In-Sync", meaning that the device is connected and that no configuration differences exist between the configuration on the physical device and the modeled configuration in NetScreen-Security Manager, or "Sync Pending", meaning that the device is unconnected and that the physical device will be updated with the modeled configuration when the device reconnects to the management system. However, if a device is connected but its configuration is not "In-Sync", the update process skips that device to avoid installing unexpected changes.

To handle unconnected devices during the update, you must also specify additional post-action options, as detailed in the table shown below.

<table>
<thead>
<tr>
<th>Post Actions</th>
<th>What It Means</th>
</tr>
</thead>
<tbody>
<tr>
<td>--none</td>
<td>Specifies that the GUI Server should update its attack object database only (the server does not update managed security devices).</td>
</tr>
<tr>
<td>--update-devices</td>
<td>Specifies that the GUI Server should update its attack object database, then update managed security devices with the new attack objects.</td>
</tr>
<tr>
<td></td>
<td>The device must be connected to the management system with an &quot;In-Sync&quot; configuration status OR unconnected with a &quot;Sync Pending&quot; configuration status.</td>
</tr>
<tr>
<td></td>
<td>If a device is connected but its configuration is not &quot;In-Sync&quot;, the update process skips that device to avoid installing unexpected changes.</td>
</tr>
<tr>
<td></td>
<td>When using this option, you must also use the unconnected-handling option.</td>
</tr>
<tr>
<td>--unconnected-handling</td>
<td>Specifies how the server should handle unconnected devices. When using this option, you must also specify one of the following:</td>
</tr>
<tr>
<td></td>
<td>--skip</td>
</tr>
<tr>
<td></td>
<td>Directs the server to skip any unconnected device (server does not update attack objects on that device).</td>
</tr>
<tr>
<td></td>
<td>--retry</td>
</tr>
<tr>
<td></td>
<td>Directs the server to try to connect to an unconnected device. When using this option, you must use the device-changed-handling option.</td>
</tr>
<tr>
<td></td>
<td>NOTE: The retry option is supported only for devices running ScreenOS 5.2 and ScreenOS 5.0.0-IDP1.</td>
</tr>
</tbody>
</table>
Managing the Attack Database

Scheduling the Update

You can perform a one-time security update using guiSvrCli.sh directly, or you can use crontab (or other scheduling utility) to configure the update to run at the intervals you desire.

Table 19: Scheduled Security Update Post Actions

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--device-changed-handling</td>
<td>Specifies what the server should do when a device connects, but has out-of-band changes applied.</td>
</tr>
<tr>
<td></td>
<td>NOTE: The device-changed-handling options are supported only for devices running ScreenOS 5.2 and ScreenOS 5.0.0-IDP1.</td>
</tr>
<tr>
<td></td>
<td>When using this option, you must also specify one of the following:</td>
</tr>
<tr>
<td>--abort</td>
<td>Directs the server to abort the update attempt. The device configuration state is set to “Both Changed”, indication that both the device and NetScreen-Security Manager have pending changes.</td>
</tr>
<tr>
<td>--override-device</td>
<td>Directs the server to update the device with the new attack objects, overwriting any out-of-band changes made to the device.</td>
</tr>
</tbody>
</table>

NOTE: Before performing or scheduling a security update, we recommend that you disable the auto-update setting for all managed devices. To disable this setting in the device configuration, from the device navigation tree, select Security > Attack DB > Settings, then set the Schedule Mode to Disable.

To perform a one-time security update:

1. Log in to the NetScreen-Security Manager GUI Server as root.
2. Change to the utility directory by typing: cd /usr/netscreen/GuiSvr/utils
3. Type the following to update attacks, including specifying the post action options for the update:

   guiSvrCli.sh --update-attacks --post-action <post-action options>

To configure a scheduled security update using cron tab:

1. Log in to the NetScreen-Security Manager GUI Server as root.
2. Change to the utility directory by typing: cd /usr/netscreen/GuiSvr/utils
3. Type the following to update attacks, including specifying the post action options for the update:

   guiSvrCli.sh --update-attacks --post-action <post-action options>

   crontab -e

   <minutes after hour> <hour> * * * guiSvrCli.sh --update-attacks --post-action <post-action options>
During the update, the guiSvrCli utility updates its the attack object database, then performs the post actions. After updating and executing actions, the system generates an exit status code of 0 (no errors) or 1 (errors).

EXAMPLE: USING CRON TAB TO SCHEDULE ATTACK UPDATES
In this example, you are running the NetScreen-Security Manager system on Linux, and you want to use cron tab to update attack objects for your managed security devices every day at 5:00am. For unconnected devices, you want to retry the update when the device connects, overwriting any out-of-band changes made to the device.

1. Log into the GUI server as root.
2. Change to the utility directory by typing: cd /usr/netscreen/GuiSvr/utils
3. Type the following commands:
   
   ```
   crontab -e
   0 5 * * * guiSvrCli.sh --update-attacks --post-action --update attacks --unconnected-handling --retry --device-changed-handling --override-device
   ```

   You can view expanded update results using the Job Manager and Audit Log Viewer in the NetScreen-Security Manager UI, as detailed in the following sections.

Viewing Scheduled Security Updates in the Job Manager
Each scheduled security update generates a Job Manager entry, entitled Scheduled Attack and Device Update. The entry contains job status information, such as “connected to server” or “no new security update available”.

If the post-action was update-attacks, the job information also includes:

- A list of devices that the server attempted to update with new attack objects.
- For each device, the status of the update, such as “update successful”, “device skipped due to pending changes”, or “update aborted”.

To view a Job Manager entry, in the main navigation tree of the NetScreen-Security Manager UI, select Job Manager then doubleclick the entry you want to view.

Viewing Scheduled Security Updates in the Audit Log Viewer
Each scheduled security update generates an entry in the Audit Log Viewer. The entry contains the following information:

- Time Generated—Specifies the time at which the update began.
- Admin Name/Domain—The admin name for security update is guiSvrCli and the domain is Global (entry appears as guiSvrCli/Global).
- Action—The action appears as “Scheduled Attack and Device Update”.

Managing the Attack Database  ■  425
To view an audit log entry, in the main navigation tree of the NetScreen-Security Manager UI, select Audit Log Viewer.

Updating AV Pattern Files

Some security devices provide antivirus (AV) scanning for specific application-layer transactions using an internal AV scanner developed by Trend Micro. The internal AV scanner references a virus pattern file to identify virus signatures. As new viruses emerge, the pattern file on the device needs to be updated.

To update the AV pattern file for a device:

1. From the menu bar, select Devices > AV Scan Manager > Update Pattern. The Update Pattern dialog box appears.
2. Select the device(s) or group of devices to be updated.
3. Click OK. The Job Information window displays the status of the update.

Updating the URL Category List

URL Categories (predefined by SurfControl) are used to create the default WEB Filtering Profile object, which you can use in a firewall rule to permit or deny specific URL requests to or from your protected network.

The SurfControl CPA server periodically updates its predefined category list, but does not notify its clients when the list is updated. To ensure that the security device and NetScreen-Security Manager use most up-to-date predefined categories, you must update the list manually, first on the device, then for the NetScreen-Security Manager system.

NOTE: The security device periodically polls the CPA server for category updates. The default interval is every two weeks; for details on changing this settings, see “Configuring Integrated Web Filtering” on page 323.

You must perform both steps listed below, in the following order:

1. In the menu bar, select Devices > WEB Filtering > Update URL Categories. This option updates the security device predefined categories from the SurfControl CPA server.
   
   You must perform this step before updating the categories on the NetScreen-Security Manager management system. When the Select Devices dialog box appears, select the security device you want to contact SurfControl.

2. In the menu bar, select Devices > WEB Filtering > Update System Categories. This option updates the NetScreen-Security Manager management system predefined categories from a security device.
   
   You must perform this step after updating the predefined categories on the security device.
Miscellaneous Device Operations

This section describes other device management tasks that you can perform using the NetScreen-Security Manager UI.

- Restarting Devices
- Refreshing DNS Entries
- Updating the Device Clock with an NTP Server
- Setting the Root Administrator on a Device
- Failing Over/Reverting Back Interfaces
- Setting RMA State on a Device
- Troubleshooting a BGP Peer Session on a Device
- Displaying CLI Commands on a Device
- Reactivating Wireless Connections
- Finding Usages

The following sections detail each management task.

Restarting Devices

You can restart one or more selected devices, or a group of devices. To restart one or more devices:

1. From the menu bar, select Devices > Reboot Device. The Reboot Device(s) dialog box appears.

2. Select the device(s) or the group of devices to be restarted.

3. Click OK. The Job Information window displays the status of the restart.

Refreshing DNS Entries

To enable a security device to use Domain Name System (DNS) to resolve domain names to IP addresses, you configure the IP addresses of the primary and secondary DNS servers on the device. The device can automatically refresh entries in its DNS table by checking them with the specified DNS server at regularly scheduled times or intervals, or after an HA failover).

You can also manually direct the device to refresh its DNS table entries. When you direct the device to refresh its DNS entries, it connects to the previously-configured DNS server to perform a lookup of each entry in its table.

To direct one or more devices to refresh their DNS table entries:

1. Select DNS > Refresh DNS Entries from the Devices menu. The Refresh DNS Entries dialog box appears.
2. Select the device(s) or the group of devices on which DNS tables should be refreshed.

3. Click OK. The Job Information window displays the status of the refresh.

**Updating the Device Clock with an NTP Server**

The security device can use the Network Time Protocol (NTP) to synchronize its system clock with a configured NTP server over the Internet. You can configure the device to perform this synchronization automatically at specific time intervals (see “Configuring Date and Time Settings” on page 308), or you can direct the device to synchronize its clock immediately to a previously-configured NTP server, as described in the following steps.

To direct one or more devices to synchronize their clocks:

1. From the menu bar, select Devices > NTP > Perform NTP Time Update. The Perform NTP Time Update dialog box appears.

2. Select the device(s) or group of devices that should be synchronized with NTP servers.

3. Click OK. The Job Information window displays the status of the synchronization.

**Setting the Root Administrator on a Device**

All security devices ship with the same default login and password for the root administrator. Because these default settings known, you should change the login and password for the root administrator as soon as possible and as often as necessary.

Each security device can have only one root administrator, who has the following privileges:

- Manages the root system of the security device
- Adds, removes, and manages all other administrators
- Establishes and manages virtual systems, and assigns physical or logical interfaces to them
- Creates, removes, and manages virtual routers
- Adds, removes, and manages security zones
- Assigns interfaces to security zones
- Performs asset recovery
- Sets the device to FIPS mode

**NOTE:** All passwords handled by NetScreen-Security Manager are case-sensitive.
- Resets the device to its default settings
- Updates the firmware
- Loads configuration files

After you change the root administrator login and password, only persons who know the new login and password can log into the device and perform the tasks listed above.

To configure the login and password for the root administrator for a security device:

1. In Device Manager, right-click a device icon select Admin > Set Root Admin. The Set Root Admin dialog box appears for the device.
2. Enter the new name in the Administrator Name field.
3. Enter the new password in the Password field and then re-enter the same password in the Confirm Password field.
4. Click OK.

For more details on managing device administrators, including the root administrator, see “Configuring Device Administrators” on page 297.

**Failing Over/Reverting Back Interfaces**

Some security devices support port modes that bind a second backup interface to the Untrust zone. For these port modes, the backup interface is used only when there is a failure on the connection through the primary interface or when you manually force traffic from the primary interface to the backup.

To force a security device to fail over to the backup interface:

1. Right-click a device from the security device Tree or the security device List tab in the Device Manager and select Admin > Failover. The Failover Action dialog box appears.
2. Click Force to Failover.
3. Click OK.

To force a security device to revert back to the primary interface:

1. Right-click a device from the security device Tree or the security device List tab in the Device Manager and select Admin > Failover. The Failover Action dialog box appears.
2. Click Force to Revert.
3. Click OK.
Setting RMA State on a Device

If you need to send a device back to the factory and replace it with a new device, you can set the device to the RMA state. This state allows NetScreen-Security Manager to retain the device configuration without a serial number or connection statistics. When you install the replacement device, all you need to do is activate the device with the serial number of the replacement unit.

NOTE: The replacement device must be the same platform and ScreenOS version as the unit that is being replaced. Setting the RMA state cannot be undone.

In the RMA state, the device object is functionally identical to a modeled device, but its status is “RMA” in the Device Monitor.

To set a device to the RMA state:

1. Right-click a device from the security device Tree or security device List tab in the Device Manager and select RMA Device. The Confirm RMA Device dialog box appears.
2. Click OK. In the Device Monitor window, the device status is RMA.

When the replacement device is installed, activate the device with the serial number of the replacement. For information about activating a device, see “Activating a Device” on page 98.

Troubleshooting a BGP Peer Session on a Device

To troubleshoot BGP peer configurations, you can connect and disconnect BGP connections to a specific neighbor. You can also test the TCP connection to a specific neighbor. To perform these tests, you need to have configured a virtual router and the BGP dynamic routing protocol on the device, and enabled BGP on the virtual router and on the interface to the BGP neighbor.

To connect or disconnect to a BGP peer:

1. In the main navigation tree, select Device Manager > Security Devices. Right-click a device and select Admin > Modify BGP Peer Session. The Modify BGP Peer Session dialog box appears.
2. Select the virtual router in which the BGP configuration resides.
3. Select the peer to which you want to connect or disconnect from the list of configured BGP neighbors.
4. Select Connect to establish a BGP connection to the selected peer, Disconnect to terminate the BGP connection to the selected peer, or TCP Connect to test the TCP connection to the selected peer.
5. Click OK.
Displaying CLI Commands on a Device

To display the CLI configuration commands for a device, right-click a device from the security device Tree or security device List tab in the Device Manager and select Admin > Show Device Commands.

Reactivating Wireless Connections

You can deploy a Juniper Networks NetScreen-5GT Wireless security device running ScreenOS 5.0.0-WLAN as a wireless access point (WAP). When you make changes to the wireless settings for the security device, you must update the device with your changes before the new settings take effect. Additionally, the device must reactivate its WLAN subsystem to use the new settings. NetScreen-Security Manager automatically reactivates the WLAN subsystem within the wireless security device during the device update process.

Finding Usages

To locate groups, vsys, policies, and VPNs that reference a specific device, right-click a device select Find Usages. The Find References box appears.

Managing Device Capabilities

This section presents a detailed description of how NetScreen-Security Manager components enable you to add, configure, update, and manage security devices. The illustration below is an overview of the components and how they interact with each other. A description of each component follows.
Abstract Data Model

The Abstract Data Model (ADM) is an XML file that contains configuration data for all objects in a specific domain. The ADM is stored in the GUI Server, but you do not access the ADM directly. When you create, update, or import a device, the GUI Server edits the ADM to reflect the changes. The Management console uses the ADM to determine the current options, fields, screens, and data range to display in the UI for each object.

Data Model

A Data Model (DM) is an XML file that contains configuration data for an individual device. The DM is stored in the Device Server. When you create, update, or import a device, the GUI Server edits the ADM to reflect the changes, then translates that information to the DM.
Data Model Schema

The structure of the ADM and DM is determined by the Data Model (DM) schema. The DM schema reads from a device capability file to determine the supported features for the ScreenOS version that is running on the managed devices. A device capability file lists the fields and attributes that a specific ScreenOS version supports.

Your network may contain similar security devices that are running different ScreenOS versions. For example, a NetScreen-5XT may run ScreenOS 5.x, which supports the Routing Information Protocol (RIP), while another NetScreen-5XT runs ScreenOS 4.0.0r2, which does not support RIP. The DM schema links to the appropriate device capability file for each device.

Device capability files make it easier to integrate devices into NetScreen-Security Manager and also make upgrading the software on your security devices easier. Each software release includes device capability files that describe the new and changed fields, attributes, and allowable ranges of values.

Data Model Updating

Data Model update is the process of translating the objects and object attributes in the ADM domain into individual DMs with device-specific configuration information.

In the ADM, objects are arranged similarly to objects in the management console: each item (VPN, policy, device, device group, and so on) is represented by an object. In the DM, each item is a property of a single device. During the data model update process, the GUI Server identifies the objects that contain properties for a device, and translates those object properties into properties of that device.

When you update a device configuration using the management console, the GUI Server translates the objects and object attributes in the ADM domain into device configuration information in a DM. The Device Server then translates the device configuration information in the DM into CLI commands and sends the commands to the device.
For example, the ADM contains a VPN with tunnel interfaces, a routing table, and users. When you update a selected device, the DM update identifies the devices that are involved in the VPN and creates interfaces, routing tables, users, and VPN rules in the DM for each device. The DM contains only the VPN information that relates to the specific device, not the entire VPN.

During the device model update process:

- The GUI Server translates the object and object attributes in the ADM domain into device configuration information in a DM.

- The Device Server translates the device configuration information in the DM into CLI commands.

- The Device Server sends the CLI commands to the device.
Data Model Importing

Data Model Import (DM import) is the process of translating the device-specific configuration information in individual DMs into the objects and object attributes in the ADM domain.

When you import a device configuration using the management console, the device sends CLI commands to the Device Server, which translates the CLI commands into a DM with device configuration information. The GUI Server then translates the device configuration in the DM into objects and object attributes in the ADM, and uses the ADM to display current information in the management console.

Figure 102: Data Model Importing

During the device model import process:

- The device sends CLI commands to the Device Server, which translates the CLI commands into a DM with device configuration information.
The GUI Server translates the device configuration in the DM into objects and object attributes in the ADM.

The GUI Server then reads the ADM and displays the current information.

Archiving and Restoring

You can archive and restore log and configuration data in NetScreen-Security Manager using standard Unix commands. Logs reside on the Device Server; all other configuration information, including device configuration data, administrators, policies, audit logs, and job information resides on the GUI Server.

Before archiving, you must stop the processes running on both servers, then use the "ls -al" command to identify the actual paths of the GUI Server and Device Server data directories:

- For all information on the GUI Server: /usr/netscreen/GuiSvr/var
- For all information on the Device Server: /usr/netscreen/DevSvr/var

These directories are links representing the paths that were entered at the time the servers where installed.

After archiving, restart the processes on both servers. For details on stopping, starting, and restarting processes on the management system, refer to the NetScreen-Security Manager 2005.3 Installer's Guide.

Archiving Logs and Configuration Data

To archive log and configuration data:

1. Stop the Device Server and the GUI Server.
2. Use the ls -al command to discover the actual paths of the GUI Server and Device Server data directories. These are the directories you need to back up.

   For example:

   ```
   ls -al /usr/netscreen/GuiSvr/var
   lrwxrwxrwx 1 root root 21 Feb 25 16:04 /usr/netscreen/GuiSvr var ->
   /var/netscreen/GuiSvr
   ```

   The output in the example indicates that the actual location of the GUI Server data is in /var/netscreen/GuiSvr. On your own system, verify where your data is stored and which directories should be backed up. Follow the same procedure to determine the location of your data on the Device Server.

3. Run the appropriate backup command on your Solaris or Linux platform to backup the GUI Server data. For example:
4. Run the appropriate backup command on your Solaris or Linux platform to backup the Device Server data.

   For a large amount of log data, using tar may not be appropriate. we recommend using Secure Copy (scp) or File Transfer Protocol (FTP) to backup the Device Server data.

   Example using scp:

   scp -r <local directory> user@host:<remote-directory>

   Example using FTP:

   ftp <host name>
   bi
   hash
   lcd <local directory>
   prompt
   mput

5. Start GUI Server and Device Server processes.

**Restoring Logs and Configuration Data**

These instructions apply only to systems where the var directory links point to a true location outside the prescribed locations (/usr/netscreen/GuiSvr or /usr/netscreen/DevSvr). We recommend that you do not set these links to point to locations that are inside /usr/netscreen/GuiSvr or /usr/netscreen/DevSvr; doing so can complicate upgrades to NetScreen-Security Manager and requires special precautions during backup and restore procedures.

To restore log and configuration data:


2. Use the mv command to transfer data from the var directories to a safe location. This precaution clears the var directory for restoration of the backups.

3. Untar your backups into both of the locations described above.

Part 3
Managing

The chapters in Part 3 of the NetScreen-Security Manager 2005.3 Administrators Guide are designed to help you create the building blocks of the management system (objects), then configure the Security Policies and VPNs that control your network traffic.

Part 3 contains the following chapters:

- Chapter 8 “Configuring Objects” details how to configure shared objects, such as address, service, schedule, attack objects, and NAT objects such as VIPs, MIPs, and DIPs.


- Chapter 10 “Configuring VPNs” details how to create VPN components such as protected resources and IKE proposals, and guides you through building VPNs at the system level and at the device level.

After you have built objects, created Security Policies that define how your devices should handle traffic to and from the firewall, and configured VPNs to connect your network security devices, your network should be configured, connected, and secure. Next, you can begin to use NetScreen-Security Manager’s monitoring, logging, and reporting features to review the status of your security devices (and VPN tunnels) and the efficiency of your firewall and multicast rules, as detailed in Part 4, “Monitoring” on page 679.
Chapter 8
Configuring Objects

Objects represent reusable information, such as network addresses, individual users and user groups, and commonly used configuration data. In NetScreen-Security Manager, objects are shared objects, meaning they are shared between the global domain and all subdomains.

Objects are the building blocks of the NetScreen-Security Manager management system. You can use an object multiple times in the same domain. For example, you can create an address object to represent a host such as an individual workstation, then use the address object in a VPN protected resource and as the source or destination in a firewall or multicast rule.

The following sections are in this chapter:

- About Objects
- Configuring Address Objects
- Configuring Schedule Objects
- Working With DI Attack Objects
- Working with IDP Attack Objects
- Configuring Custom DI/IDP Attacks
- Creating Custom DI Attack Groups
- Configuring AntiVirus Objects
- Configuring Web Filtering Objects
- Configuring GTP Objects
- Configuring Service Objects
- Configuring Authentication Servers
- Configuring User Objects
- Configuring IP Pools
- Configuring Group Expressions
- Configuring Remote Settings
- Configuring NAT Objects
- Configuring Certificate Authorities
- Configuring CRL Objects
- Configuring Protected Resources
- Configuring IKE Proposals
About Objects

Within the NetScreen-Security Manager UI, most objects appear in Object Manager, and VPN-related objects under VPN Manager. For some object types, such as service objects, attack objects, and IKE proposal objects, predefined objects exist. For most object types, however, you must configure an object before you can use it in your device configuration or Security Policies.

NOTE: If you imported an existing device configuration, NetScreen-Security Manager automatically imported all objects defined in the running device configuration.

Object Manager displays objects created in the current domain only. When working in the global domain, all custom objects are viewable. When working in a subdomain, only custom objects created in the subdomains are viewable. However, when creating an object group, you can select objects from both the current subdomain and global domain. Any global object that is part of a subdomain object group appears within the subdomain object list.

Use Object Manager to view and configure the following objects:

- Host and network addresses:
  - Address Objects represent individual hosts or subnetworks in your network.
  - NAT Objects (DIP, MIP, VIP) represent references to device-specific NAT configurations (dynamic IPs, mapped IPs, and virtual IPs), enabling multiple devices to share a single object.
  - IP Pools define ranges of IP addresses used to assign an IP address to a RAS user.
  - Remote Settings represents DNS and WINS servers.

- Services and schedules:
  - Schedule Objects represent time periods and determine when a rule is in effect.
  - Service Objects represent predefined and custom network services, such as HTTP/80.

- Application Layer Protection:
  - DI Profiles define the attack signature patterns, protocol anomalies, and the action you want a security device to take against matching traffic.
  - AV Profiles define the server that contains your virus definitions and Antivirus software.
  - Web Filtering Profiles define the URLs, the URL categories, and the action you want a security device to take against matching traffic.

- Users and Authentication:
User Objects represent RAS users on your network.

Authentication Servers represent the servers in your network used to authenticate NetScreen-Security Manager admins, RAS users, and network traffic.

Group Expressions define logical expressions used to include or exclude RAS users.

Certificates:

- Certificate Authority Objects represent the certificate authority’s certificate.
- CRL Objects represent the certificate authority’s certificate revocation list.

VoIP Protection:

- GTP Objects represent client GTP configurations.

Use VPN Manager to view and configure the following objects:

- Protected Resources represent the network components, a network service, and the security device that protects those components and service.
- IKE Phase1 Proposals represent the phase1 proposals used to establish a secure and authenticated communication channel between two VPN members.
- IKE Phase2 Proposals represent the Security Associations for services (such as IPsec) that require key material and/or parameters, as exchanged by two VPN members.

Importing Objects from Global-PRO

If you already have objects defined in your existing Juniper Networks NetScreen-Global PRO management system or on the device itself, you can import those objects into NetScreen-Security Manager.

When importing device configurations and their domains from Global PRO, NetScreen-Security Manager also imports all objects that are defined for those domains. During this import process, NetScreen-Security Manager determines if the object is accessible by a single domain or accessible by all domains.

For details on importing objects from Global-PRO, refer to the NetScreen-Security Manager Migration and Installer’s Guide.

Using Objects Across Domains

Objects created in the global domain are available in all subdomains, but objects created in a subdomain are only available in that subdomain.

For example, when creating a VPN:

- You can use a global domain user object in a subdomain VPN.
- You can use a subdomain user object in a subdomain VPN.
You cannot use a subdomain user object in a global domain VPN.

When creating a subdomain protected resource, you can include a subdomain address object and a global domain service object, but you can only select the protected resource when you are logged in to that specific subdomain.

### Configuring Address Objects

An address object is a representation of a component of your network, such as a workstation, router, switch, subnetwork, or any other object that is connected to your network. You use address book objects in NetScreen-Security Manager to specify the network components you want to protect:

- **Firewall and IDP Rules**—Use address objects or groups to specify the source and/or destination of network traffic.
- **Multicast Rules**—Use multicast group address objects to specify the destination of multicast traffic.
- **VPNs**—Use address objects or groups to create Protected Resources for your Policy-Based and Mixed-Mode VPNS.

### Viewing Address Objects

In the navigation tree, click Object Manager > Address Objects to view all address objects for the current domain. You can display Address objects in a tree or table format:

- The Address Tree tab displays address objects in a tree format. To view the members of an Address Object group, click the group to display a member list.
- The Address Table tab displays address objects in a table format with the following columns:
  - Name—Name of the address object
  - Type—Type of the address object (Host, Network, Group)
  - IP/Domain Name—The IP address or host name (such as www.juniper.net) of the address object
  - Netmask—Netmask of the address object
  - Comment—A description of the address object

When you initially deploy the NetScreen-Security Manager system and open the UI for the first time, the Address Object tree and table tabs are empty. Using the Object Manager, you can create Address Objects that represent network components that are unique to your network. As you add address objects, they appear in the tree and table tabs.
Creating Address Objects

You can create the following address objects:

- **Host**—Represents components, such as workstations, connected to your network.
- **Network**—Represents divisions or subnetworks in your network.
- **Address Object Group**—Represents multiple address objects.
- **Multicast Group**—Represents the destination of multicast packets.

The following sections detail each Address Object type.

Adding a Host Address Object

To add a host address object:

1. In the navigation tree, select Object Manager > Address Objects. The address object tree appears. In the main display area, click the add icon and select Host.

2. Enter a unique name for the address object and select a color to represent the address object.

3. Enter a Comment about the host.

4. Enter the address that identifies the host on your network:

   - To identify the host with an IP address, select IP and enter the IP address of the host. Click Resolve to automatically resolve the domain name for that IP address.
   - To identify the host with a domain name, select Domain Name and enter the domain name of the host. Click Resolve to automatically resolve the IP address for that domain name.

5. Click OK to add the address object.

The new host address object immediately appears in the Address Tree and Address Table.

Adding a Network Address Object

To add a network address object:

1. In the navigation tree, open the Object Manager and select Address Objects. The address object tree appears. In the main display area, click the add icon and select Network.

2. Enter a name for the address object.

3. Enter the IP address and netmask of the network.

4. Select a color to represent the address object.
5. Enter a Comment about the network, then click OK to add the address object.

The new network address object immediately appears in the Address Tree and Address Table.

Adding an Address Object Group

To simplify your Security Policies, you can combine multiple address objects in an address object group. An address object group can contain address objects (and other address object groups) from current subdomain and the global domain.

To add an Address Object Group:

1. In the navigation tree, open the Object Manager and select Address Objects. The address object tree appears. In the main display area, click the add icon and select Group.

2. Enter a unique name for the group.

3. Select a color to represent the group.

4. Enter a Comment about the group.

5. In the Non-members list, select the address objects you want to include in the group (hold down Ctrl to select multiple address objects):

   - If you are in the global domain, only the global address objects appear in the non-members list.
   - If you are in a subdomain, both global and subdomain address objects appear in the non-members list.

6. Click Add. The selected address objects now appear in the member list.

7. Click OK to add the group.

You can create address object groups with existing users or create empty address object groups and fill them with users later.

Adding a Multicast Group Address Object

To add a multicast group address object:

1. In the navigation tree, open the Object Manager and select Address Objects. The address object tree appears. In the main display area, click the add icon and select Multicast Group. The New Multicast Group dialog box appears.
2. Enter a name for the multicast group address.

---

**NOTE:** Multicast Group address object names must be unique; you cannot name a multicast group address object the same name as an existing multicast group address object.

3. Select a color to represent the multicast group address.

4. Enter a Comment about the multicast group address.

5. Enter the IP address of the multicast group.

6. Click OK to add the multicast group address.

---

**Adding Static DNS Host Addresses**

This ScreenOS 5.3 feature lets you create a static host name with multiple IP addresses. You can use this feature to create dynamic addressing in NSM.

To add multiple static host addresses:

1. In the navigation tree, open Device Manager and click Security Devices.

2. Double-click the device you want to configure. The device must be running ScreenOS 5.3 or later.

3. In the navigation tree of the new dialog box, open Network, then DNS.

4. Click Settings to open the Device Settings dialog box.

5. Click the add (plus sign) icon, enter the host name and host IP address, then click OK.

6. Click OK to save the changes and close the dialog box.
Configuring Schedule Objects

Example

In some cases, a common firewall policy is desired but due to differences in the IP addressing at different sites, it is impossible to share the policy. Using the static host entries and address objects, this can be accomplished. Each device would contain a local mapping of hostname to IP, but the policy would contain address object referencing the hostname. This allows the firewall policy to focus on the application as opposed to the specific IP addressing.

For example, each site may have a web server, each with different IP addresses. By defining an address object using the hostname "webserver" and then using that object in the firewall policy, the device will resolve the address object's hostname to the correct IP for that device (as defined by the static host entry on the device).

1. In the navigation tree, open Object Manager and click Address Objects.
2. Click the add (plus sign) icon then select Host to open the New Host dialog box.
3. Enter the same name in the Name field that you entered for the Device host name in the previous section. These values are case sensitive and must match exactly.
4. Click OK to save the name and close the dialog box.
5. Return to the navigation tree, open Security Policy.
6. Click the add (plus sign) icon and enter the security policy name, then click OK.
7. Double-click the name of the security policy you just created.
8. Right-click the value in the Source column or the Destination column.
9. Select the address object you just created, click Add, then click OK. When the address object is pushed to a device, the host name is resolved dynamically. One policy can be assigned to multiple devices.

A schedule object defines a time interval that a firewall rule is in effect. You use a schedule object in your firewall rule to determine when a device enforces that rule:

- Use a one-time schedule to control access to a destination for a specific time interval. The schedule object defines a start time, end time, and date during which a rule is enforced. Some examples:
  - Contractor Access Schedule (8:30 AM December 1 to 6:00 PM December 5)
  - Christmas Break Schedule (6:00 PM December 24 to 8:00 AM January 2)

- Use a recurring schedule to control access to a destination for a repeating time interval. The schedule object defines a start time, end time, and days during which a rule is enforced. Some examples:
  - Business Hours Schedule (8:00 AM to 6:00 PM on Monday, Tuesday, Wednesday, Thursday, Friday)
Creating Schedule Objects

To add a schedule object:

1. In the navigation tree, open the Object Manager and select Schedule Objects. The schedule object tree appears.
2. In the main display area, click the add icon.
3. Enter a name and comment for the schedule object.
4. Select the frequency of the schedule:
   - To configure a one-time schedule, select Once, and enter the Start Date, Start Time, Stop Date, and Stop Time.
   - To configure a recurrent schedule, select Recurrent, and click the Add icon. In the Recurrent Schedule dialog box, select the day of the week and specify the hour and minutes for Start 1 and Stop 1.

   To specify a second recurring time interval on the same day, specify the hour and minutes for Start 2 and Stop 2. Ex. Business Hours Schedule (8:00 to 12:00 and 13:00 to 17:00 every weekday).

Working With DI Attack Objects

Deep Inspection (DI) attack objects contain attack patterns and protocol anomalies for known attacks and unknown attacks that attackers can use to compromise your network. However, DI attack objects don’t work on their own—they need to be part of an attack object group, then a DI Profile object before you can use them in a firewall rule to detect known attacks and preventing malicious traffic from entering your network.

NOTE: Deep Inspection is supported by NetScreen-5GT devices, the NetScreen-HSC, and all devices running ScreenOS 5.x.

To create the Deep Inspection (DI) Profile object, you add predefined attack object groups (created by Juniper Networks) and/or your own custom attack object groups to the Profile object. After creating the DI Profile, you add the Profile object in the Rule Option column of a firewall rule. If an attack is detected, the device generates an attack log entry that appears in the Log Viewer.
For details on creating your own custom attack objects and custom attack object groups, see “Working With DI Attack Objects” on page 449. For more details on configuring Deep Inspection in a firewall rule, see “Creating DI Profiles” on page 451. For details on attack log entries, see “Deep Inspection Alarm Log Entries” on page 834.

**Viewing Predefined DI Attack Objects**

NetScreen-Security Manager contains a database of hundreds of predefined DI attack objects designed to protect networks from multiple attack vectors. For your convenience, we organize these attack objects into predefined groups, which you can use in a DI Profile to match traffic against known and unknown attacks.

---

**NOTE:** NetScreen-Security Manager displays a superset of all predefined DI attack objects. Based on the platform and ScreenOS firmware version, security devices include a specific subset of DI attack objects. Therefore, the list of predefined DI attack objects displayed in the NetScreen-Security Manager UI might not match the list of predefined DI attack objects on the physical security device.

---

To view individual predefined attack objects, in Object Manager, select Attack Objects > DI Objects. The Predefined Attacks tab (default view) displays a table of predefined attack objects that represent known and unknown attack patterns. Use the Predefined Attacks tab to quickly view details about an attack object, such as name of the attack object, attack severity, attack category, and attack references. To view the properties for an attack, right-click the attack and select View.

To locate all firewall rules that use a predefined attack object or group, right-click the attack object and select View Usages.

**Viewing Attack Version Information for Attack Objects**

You can view details for predefined attack objects; however, not all details are applicable to all attacks.

The Pattern field under the Detection tab in the Attack Version dialog box contains the regular expression used to identify the attack. Juniper Networks Security Engineering might choose to hide the exact pattern for specific attack objects. This is done to protect the confidentiality of either the source or target of the specific attack object. In such cases, the field displays Protected instead of the regular expression.

To view attack version information, click one of the Supported Platform links within an attack object dialog box.

**Viewing Predefined DI Attack Object Groups**

To view predefined attack object groups, in Object Manager, select Attack Objects > DI Objects, then select the Predefined Attack Groups tab. The name of each attack object group indicates the severity, protocol, and attack type of the individual attack objects contained within. For example, the predefined attack object group CRITICAL:DNS:ANOMALY contains predefined protocol anomaly attack objects that detect critical Domain Name Service (DNS) attacks.
To locate all firewall rules that use a predefined attack object or group, right-click the attack object group and select View Usages.

**Updating Predefined DI Attack Objects and Groups**

You cannot create, edit, or delete predefined DI attack objects or groups, but you can update the attack object database with new attack object created by Juniper Networks. Updates can include:

- New descriptions or severities for existing attack objects
- New attack objects
- Deletion of obsolete Attack Objects

For details on managing the attack object database, see “Managing the Attack Database” on page 415.

**Creating DI Profiles**

A Deep Inspection (DI) Profile object contains predefined attack object groups (created by Juniper Networks), and/or your own custom attack object groups. After creating the DI Profile, you add the Profile object in the Rule Option column of a firewall rule.

To create a DI Profile, in the navigation tree, select Object Manager > Attack Objects > DI Objects, then click the Profile tab. Click the Add icon to add a new Profile object, then configure the name, color, and comments for profile object as desired. To add members to the profile object, configure the following:

- **DI Severity Setting**—Select a DI Severity setting for the profile object. The DI Severity setting overrides the severity setting of the attack objects included in each profile member.

- **Signature Category**—Select a category of DI signatures. You can only select categories for which you have a license.

Categories are as follows:

- **Server Protection Pack**—Designed to protect servers.
- **Client Protection Pack**—Designed to protect remote and home offices.
- **Worm Mitigation Pack**—Designed to protect against worms.
- **Base (Default) Pack**—All signatures. May be too large for some devices.

- **DI Attack Objects and Groups**—Add a profile member to the profile object. Each profile member can contain attack object groups, and you can add multiple profile members to the profile object. Within each profile member:

  - Select the attack object groups you want to include in this profile member.
Configure the action you want the security device to take when an attack object within the profile member matches traffic. For each attack that matches a rule, actions respond to matching traffic using one of the following actions:

Table 20: Deep Inspection Profile Actions

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>The security device takes no action against the connection.</td>
</tr>
<tr>
<td>ignore</td>
<td>The security device ignores the remainder of a connection after an attack object is matched.</td>
</tr>
<tr>
<td>drop packet</td>
<td>The security device drops a matching packet before it can reach its destination but does not close the connection. Use this action to drop packets for attacks in traffic that is prone to spoofing, such as UDP traffic. Dropping a connection for such traffic could result in a denial of service that prevents you from receiving traffic from a legitimate source IP address. For TCP connections, dropping a single packet will result in the same packet being resent. So, Drop Packet settings are translated to Drop Connection settings for TCP connections.</td>
</tr>
<tr>
<td>drop connection</td>
<td>The security device drops the connection without sending a RST packet to the sender, preventing the traffic from reaching its destination. Use this action to drop connections for traffic that is not prone to spoofing.</td>
</tr>
<tr>
<td>close client and server</td>
<td>The security device closes the connection and sends a RST packet to both the client and the server.</td>
</tr>
<tr>
<td>close client</td>
<td>The security device closes the connection to the client, but not to the server.</td>
</tr>
<tr>
<td>close server</td>
<td>The security device closes the connection to the server, but not to the client.</td>
</tr>
</tbody>
</table>

NOTE: Network security is an ongoing process of understanding what is normal traffic for your network. Eliminating malicious traffic is important, but identifying ambiguous traffic can be equally important. You do not always want to drop traffic that appears abnormal; you might want to reset the connection, block the attacker, simply set an alert for the event, or use all three methods.

Configure Deep Inspection Alerts. Enable this option to create an event log entry for matching traffic. If the security device matches network traffic to an attack object in the rule, NetScreen-Security Manager creates an event log entry that describes that attack (direction, service, and Attack object) and displays an alert in the Log Viewer.

Configure IP Action. Enable this option to direct the device to take action against a brute force attack. When enabled, configure the following IP controls action:

- Action. Select the action you want the device to take when it detects a brute force attack.
### Table 21: Deep Inspection IP Actions

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Block</td>
<td>The security device logs the event and drops all further traffic matching the target definition for the period of time specified in the timeout setting.</td>
</tr>
<tr>
<td>IP Close</td>
<td>The security device logs the event and drops all further traffic matching the target definition for the period of time specified in the timeout setting, and sends a Reset (RST) for TCP traffic to the source and destination addresses.</td>
</tr>
<tr>
<td>IP Notify</td>
<td>The security device logs the event but does not take any action against further traffic matching the target definition for the period of time specified in the timeout setting.</td>
</tr>
</tbody>
</table>

- **Target**: Specifies a set of elements that must match for the security device to consider a packet part of a brute force attack. The specified set of elements in an IP packet arriving during a specified timeout period must match that in the packet that the security detected as part of a brute force attack for the subsequent packet to be considered part of the same attack. Possible values are Source, Destination, Destination Port and Protocol; Source; Destination; From Zone, Destination, Destination Port and Protocol; and From Zone.

- **Timeout (sec)**: A period of time following brute force attack detection during which the security device performs an IP action on packets matching specified target parameters. The default is 60 seconds.

After you have created the DI Profile object, you can use the object in your firewall rules. For details, see “Configuring a DI Profile/Enable IDP For Firewall Rules” on page 551.

### Working with IDP Attack Objects

NetScreen-Security Manager contains a database of predefined IDP attack objects and IDP attack object groups that you can use in Security Policies to match traffic against known and unknown attacks. Juniper Networks updates the predefined attack objects and groups on a regular basis with newly-discovered attack patterns.

### Viewing Predefined IDP Attacks

The Predefined Attacks tab displays all attacks in a table format and includes the following information:

- **Name of the attack object**
- **Severity of the attack**: critical, major, minor, warning, info
- **Category**
- **Keywords for the attack**
- **CVE number which identifies the attack’s number in the Common Vulnerabilities and Exposures database**
Bugtraq number which identifies the equivalent attack in the Security Focus Bugtraq database

By default, attack objects are listed alphabetically by Category name. To view attacks in different order, click a column heading. To display a detailed description of an attack object, double-click the attack.

To locate all rules that use a predefined attack object, right-click the attack object and select View Usages.

Figure 103: Attack Viewer

FTP Exploit: Bounce Attack

This protocol anomaly is an FTP bounce attack. There are two possibilities: a PONT command specified an IP address different from the client address, or a PASV command resulted in a 227 message with an IP address different than the server.

Details

- severity
  - Major
- category
  - FTP
- keywords
  - Not available.
- short name
  - FTP:EXPLOIT:BOUNCE-ATTACK
- supported platforms
  - [sos5.0.0] [sos5.1.0] [idp3.0r2] [idp3.1]
- last modified
  - 2003-04-22

References

- http://online.securityfocus.com/bid/126/disussion/
- http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0017

Extended Description

Impact

Not available.

Description

Not available.

Technical Information

Not available.
Viewing Predefined IDP Attack Groups

The Predefined Attack Group tab displays the following predefined attack groups:

- **Category** groups attack objects by predefined categories. Within each category, attack objects are grouped by severity.

- **Operating System** groups attack objects by the operating system to which they apply: BSD, Linux, Solaris, or Windows. Within each operating system, attack objects are grouped by services and severity.

- **Severity** groups attack objects by the severity assigned to the attack. IDP has five severity levels: Info, Warning, Minor, Major, Critical. Within each severity, attack objects are grouped by category.

To locate all rules that use a predefined attack object group, right-click the attack object group and select View Usages.

A predefined static group can include the following members:

- Predefined attack objects
- Predefined static groups
- Predefined dynamic groups

To display a detailed description of an attack object group, double-click the attack.

Viewing Attack Version Information for Attack Objects and Groups

NetScreen-Security Manager lets you look at the details of predefined attack objects and groups. Not all details are applicable to all attacks.

The Pattern field under the Detection tab in the Attack Version dialog box contains the regular expression used to identify the attack. Juniper Networks Security Engineering may choose to hide the exact pattern for specific attack objects. This is done to protect the confidentiality of either the source or target of the specific attack object. In such cases, the field displays Protected instead of the regular expression.

To view attack version information, click one of the Supported Platform links within an attack object dialog box.

Updating Predefined IDP Attack Objects and Groups

Juniper Networks updates the predefined attack objects and groups on a regular basis with newly-discovered attack patterns. You can update the attack object database on your security devices by downloading the new attacks and groups to the NetScreen-Security Manager GUI Server, then installing the new database on your devices.

**NOTE:** You cannot create, edit, or delete predefined attack object or groups.

Updates to the attack object database can include:
Configuring Custom DI/IDP Attacks

You can create custom DI and IDP attack objects to detect new attacks or customize existing attack objects to meet the unique needs of your network. For example, you might want to edit the context of a custom attack object that is producing too many false positives on your network, or create a new custom attack object to detect the latest virus or Trojan that is sweeping the Internet.

The attack object creation process is similar for custom DI and IDP attack objects. To create both object types, you use the Attack Object Wizard to enter attack object information, attack pattern, and other important information. After you have configured the object however, you use each object differently:

- To use a custom DI attack object to protect your network, you must add the object to a custom attack object group and then a DI Profile object, which you then select within the Rule Options of a firewall rule. For details on creating a custom attack object group, see “Creating Custom IDP Attack Groups” on page 474. For details on creating a DI Profile object, see “Creating DI Profiles” on page 451.

- To use a custom IDP attack object to protect your network, you can simply add the attack object in an IDP rule.

Using the Attack Object Wizard

To help you create custom attack objects, NetScreen-Security Manager UI uses a Custom Attack Object wizard to guide you through each step. During the creation process, the wizard prompts you for:

- Attack Object information—You must supply an attack object name and configure the target platforms that support the attack object. You can also create an attack description, enter attack references, and set a severity for the attack object, if desired. The following sections detail the general attack object information fields.

- Attack Version information—After you have selected the target platforms, you must supply information about the attack version, including the protocol and context used to perpetrate the attack. When the attack is considered malicious, the direction and flow of the attack, the signature pattern of the attack, and the values found in the header section of the attack traffic.

To create a custom attack object, from the main navigation tree, select Object Manager > Attack Objects > DI Objects or IDP Objects, then select the Custom Attacks tab. Click the Add icon to display the custom attack object wizard.
The following sections detail the attack object creation process; for step-by-step instructions on creating a custom attack objects, see the NetScreen-Security Manager Online Help topic “Creating Custom Attack Objects”.

Configuring Attack Name and Description

In the Attack Name and Description tab, enter basic information about the attack, such as the attack object name and attack severity. You can also enter additional information, such as a general description and keywords, which can make it easier for you to locate and maintain the attack object as you use it in your firewall rules. Specifically, the attack object wizard prompts you for the following:

- Name—Enter an alphanumeric name for the object. You might want to include the protocol the attack uses in the attack name.
- Description—Enter important information about the attack, such as why you created the attack object, how the attack or exploit works, and what specific systems on your network the attack object is intended to protect. For example, you might want to include the following information:
  - Attack type (buffer overflow, password exploit, format string attack, denial-of-service)
  - Affected system (hardware, operating system, software application, or protocol the attack targets)
  - Attack mechanism (how the attack works)
  - Attack lethality (the consequences of a successful attack)

You are not required to include all this information when creating a new custom Attack Object, but it's a good idea. If you ever need to edit this attack object, the description can help you remember important information about the attack.

- Severity—Select the severity that matches the lethality of this attack on your network. Severity categories, in order of increasing lethality, are: info, warning, minor, major, critical. Critical attacks are the most dangerous—typically these attacks attempt to crash your server or gain control of your network. Informational attacks are the least dangerous, and typically are used by network administrators to discover holes in their own security system.
- Category—Enter the category to which the attack object belongs.
- Keywords—Enter descriptive words or numbers associated with the attack. Later, after you have added the custom attack object to the database, you can search using these keywords to quickly locate the attack.

When you have completed entering the basic attack information, you are ready to enter the extended attack information, as detailed below.
Configuring Extended Information

In the Extended Information tab, enter specific information about the attack. Specifically, the attack object wizard prompts you for the following:

- **Impact**—Enter details about the impact of a successful attack, including information on system crashes and access granted to the attacker.

- **Description**—Enter details about how the attack works. You might also consider adding information on the attack history (such as how it attacked your network and what steps you took to neutralize the threat).

- **Tech Info**—Enter details on the vulnerability, the commands used to execute the attack, which files are attacked, registry edits, and other low-level information.

- **Patches**—List any patches available from the product vendor, as well as information on how to prevent the attack. You might find this information in a network security advisory or from the product vendor itself.

---

**NOTE:** Use HTML tags to include a hyperlink within the text.

When you have completed entering the extended attack information, you are ready to enter the external references, as detailed below.

Configuring External References

In the External References tab, enter the external references you used when researching the attack. External references are links to the security community’s official descriptions of an attack. Because the security community is continually discovering and analyzing new attacks, and communicating their findings to each other on the Internet, references to their work are often the best way to truly understand an attack.

If you used external references when researching the attack, you should include that information in the attack object. These references, in conjunction with standard network security references, can help other admins get more detailed information about how an attack works or help you research and compare the attack in relation to a suspected new attack.

Specifically, the attack object wizard prompts you for the following:

- **URLs**—Enter up to three URLs for external references you used when researching the attack.

- **Standard References**—Enter the standardized network security organizations’ attack designations for the attack:
  
  - **CVE** (Common Vulnerabilities and Exposures) is a standardized list of vulnerabilities and other information security exposures. The CVE number is an alphanumeric code, such as CVE-1999-0003
BugTraq is a moderated mailing list that discusses and announces computer security vulnerabilities. The BugTraq ID number is a three-digit code, such as 831 or 120.

When you have completed entering the external references for the attack, you are ready to select the target platforms for the attack object, as detailed below.

**Configuring Target Platforms**

In the Target Platform tab, you must select the target platform, configure the attack version, then set a direction filter (described on page 473) for the attack object. To select the target platform and configure the attack version, click the Add icon to display the Attack Version Wizard.

First, you must select the ScreenOS or IDP versions for which the attack object is designed. Because different versions of ScreenOS and IDP support additional functionality than previous versions, you must specify the versions that must support the attack object.

To configure the selected target platform, click the Add icon to display the New Supported Platform dialog box. Select the versions of ScreenOS (sos5.0.0, sos5.1.0, sos5.2.0) or IDP (idp3.0) that must support the attack object. After you have made your selection, the attack object wizard automatically removes options from the custom attack object creation process based on the selected target platforms.

Next, select the type of attack that the attack object detects. After you have added the supported platform to the custom attack object, you can configure the attack type on that platform. Select from one of the following attack types:

- **Signature Attack Object**—(DI and IDP attack objects) A signature attack object uses a stateful attack signature (a pattern that always exists within a specific section of the attack) to detect known attacks. Stateful signature attack objects also include the protocol or service used to perpetrate the attack and the context in which the attack occurs. If you know the exact attack signature, the protocol, and the attack context used for a known attack, select this option. For continuing details on creating a signature attack object, see “Creating a Signature Attack Object” on page 460.

- **Protocol Anomaly Attack Object**—(IDP attack objects only) A protocol anomaly attack object detects unknown or sophisticated attacks that violate protocol specifications (RFCs and common RFC extensions). You cannot create new protocol anomalies, but you can configure a new attack object that controls how the security device handles a predefined protocol anomaly when detected. If you don’t know that exact attack signature, but you do know the protocol anomaly that detects the attack, select this option. For continuing details on creating a protocol anomaly attack object, see “Configuring a Protocol Anomaly Attack Object” on page 470.
● Compound Attack Object—(IDP attack objects only) A compound attack object detects attacks that use multiple methods to exploit a vulnerability. This object combines multiple signatures and/or protocol anomalies into a single attack object, forcing traffic to match all combined signatures and/or anomalies within the compound attack object before traffic is identified as an attack. By combining and even specifying the order in which signatures or anomalies must match, you can be very specific about the events that need to take place before the security device identifies traffic as an attack. For continuing details on creating a compound attack object, see “Configuring a Compound Attack Object” on page 471.

If you need to detect an attack that uses several benign activities to attack your network, or if you want to enforce a specific sequence of events to occur before the attack is considered malicious, select this option.

Click Next to configure the attack version information for the signature attack object. You must enter some general information about attack version and specific details about the attack pattern, such as the protocol and context used to perpetrate the attack. When using a packet-related context, you can also define IP settings and protocol header matches for the attack version.

Creating a Signature Attack Object

When you configure a signature attack object, you enter important information about the protocol and context used to perpetrate the attack, when the attack is considered malicious, the direction and flow of the attack, the signature pattern of the attack, and the values found in the header section of the attack traffic.

Configuring General Attack Properties

In the general properties screen, you can define the false positive frequency for the attack version, the service that the attack uses to enter your network, and the time parameters (scope and count) that determine when a traffic abnormality is identified as an attack. The following sections detail the attack version general properties.

Configuring False Positives

Select a false positive setting that indicates the frequency (unknown, rarely, occasionally, frequently) the attack object produces a false positive on your network. Although you might now have this information when you initially configure the custom attack object, as you fine-tune your system to your network traffic you can change this setting to help you track false positives.

Configuring Service Binding (IDP Attack Objects Only)

For IDP attack objects, select the service that the attack uses to enter your network. You must select a service other than “Any” if you want to chose a service context for the attack object.

NOTE: For DI attack objects, you do not select a service binding.
Any—if you are unsure of the correct service, select Any and DI attempts to match the signature in all services. Because some attacks use multiple services to attack your network, you might want to select the Any service binding to detect the attack regardless of which service the attack chooses for a connection.

IP—if you can not sure of the correct service, but know the IP protocol type, select IP protocol type for the service binding. You can specify the name of the protocol type, or the protocol type number. If you select IP as the service type, you should also specify an attack pattern (in the Detection area) and IP settings values (in the IP area). Additionally, if you use a context binding of first packet, you must leave the attack pattern empty. The supported protocol types are shown below:

Table 22: IP Protocol Name and Type Numbers

<table>
<thead>
<tr>
<th>Protocol Name</th>
<th>Protocol Type Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP</td>
<td>2</td>
</tr>
<tr>
<td>IPIP</td>
<td>4</td>
</tr>
<tr>
<td>EGP</td>
<td>8</td>
</tr>
<tr>
<td>PUP</td>
<td>12</td>
</tr>
<tr>
<td>TP</td>
<td>29</td>
</tr>
<tr>
<td>IPV6</td>
<td>41</td>
</tr>
<tr>
<td>ROUTING</td>
<td>43</td>
</tr>
<tr>
<td>FRAGMENT</td>
<td>44</td>
</tr>
<tr>
<td>RSVP</td>
<td>46</td>
</tr>
<tr>
<td>GRE</td>
<td>47</td>
</tr>
<tr>
<td>ESP</td>
<td>50</td>
</tr>
<tr>
<td>AH</td>
<td>51</td>
</tr>
<tr>
<td>ICMPV6</td>
<td>58</td>
</tr>
<tr>
<td>NONE</td>
<td>59</td>
</tr>
<tr>
<td>DSTOPTS</td>
<td>60</td>
</tr>
<tr>
<td>MTP</td>
<td>92</td>
</tr>
<tr>
<td>ENCAP</td>
<td>98</td>
</tr>
<tr>
<td>PIM</td>
<td>103</td>
</tr>
<tr>
<td>COMP</td>
<td>108</td>
</tr>
<tr>
<td>RAW</td>
<td>255</td>
</tr>
</tbody>
</table>

ICMP, TCP, and UDP—Attacks that do not use a specific service might use a specific protocol to attack your network. Some TCP and UDP attacks use standard ports to enter your network and establish a connection; to detect these attacks, configure the firewall rule that contains this attack object to monitor traffic on the standard service port or ICMP ID.
- **RPC**—The remote procedure call (RPC) protocol is used by distributed processing applications to handle interaction between processes remotely. When a client makes a remote procedure call to an RPC server, the server replies with a remote program; each remote program uses a different program number. To detect attacks that use RPC, configure the service binding as RPC and specify the RPC program ID.

- **Service**—Most attacks use a specific service to attack your network. If you select Service as the service binding, you must select the specific service used to perpetrate the attack. Additionally, you are restricted to general attack contexts (packet, first packet, stream, stream 256, or line context). To detect these attacks, configure the service binding to match the attack service.

**Supported Services:**

Table 23: Supported Services for Service Bindings

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
<th>Default Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIM</td>
<td>AOL Instant Messenger</td>
<td></td>
</tr>
<tr>
<td>Chargen</td>
<td>Chargen</td>
<td>TCP/19, UDP/19</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
<td></td>
</tr>
<tr>
<td>Discard</td>
<td>Discard</td>
<td>TCP/9, UDP/9</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name Service</td>
<td>TCP/53, UDP/53</td>
</tr>
<tr>
<td>Echo</td>
<td>Echo</td>
<td>TCP/7, UDP/7</td>
</tr>
<tr>
<td>Finger</td>
<td>Finger Information Protocol</td>
<td>TCP/79, UDP/7</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
<td>TCP/21, UDP/21</td>
</tr>
<tr>
<td>Gnutella</td>
<td>Gnutella</td>
<td></td>
</tr>
<tr>
<td>Gopher</td>
<td>Gopher</td>
<td></td>
</tr>
<tr>
<td>HTTP</td>
<td>Hypertext Transfer Protocol</td>
<td>TCP/80, UDP/80</td>
</tr>
<tr>
<td>ICMP</td>
<td>Internet Control Message Protocol</td>
<td></td>
</tr>
<tr>
<td>IDENT</td>
<td>IDENT</td>
<td>TCP/113</td>
</tr>
<tr>
<td>IMAP</td>
<td>Internet Message Access Protocol</td>
<td>TCP/143, UDP/143</td>
</tr>
<tr>
<td>IRC</td>
<td>Internet Relay Chat</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
<td></td>
</tr>
<tr>
<td>Ipr</td>
<td>Line Printer spooler</td>
<td></td>
</tr>
<tr>
<td>MSN</td>
<td>Microsoft Instant Messenger</td>
<td></td>
</tr>
<tr>
<td>NBName</td>
<td>NetBios Name Service</td>
<td>UDP/137 (NBName)</td>
</tr>
<tr>
<td>NBDS</td>
<td>NetBios Name Service</td>
<td>UDP/138 (NBDS)</td>
</tr>
<tr>
<td>NFS</td>
<td>Network File System</td>
<td></td>
</tr>
<tr>
<td>nntp</td>
<td>Network News Transfer Protocol</td>
<td></td>
</tr>
<tr>
<td>NTP</td>
<td>Network Time Protocol</td>
<td></td>
</tr>
<tr>
<td>POP3</td>
<td>Post Office Protocol, Version 3</td>
<td>TCP/110, UDP/110</td>
</tr>
<tr>
<td>Portmapper</td>
<td>Portmapper</td>
<td>TCP/111</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Remote Authentication Dial In User Service</td>
<td></td>
</tr>
<tr>
<td>rexec</td>
<td>Rexec</td>
<td></td>
</tr>
</tbody>
</table>
Configuring Custom DI/IDP Attacks

Chapter 8: Configuring Objects

Configuring Time Binding

Use Time Binding to configure the time attributes for the custom attack object. Time attributes control how the attack object identifies attacks that repeat for a certain number of times. By configuring the scope and count of an attack, you can detect a sequence of the same attacks over a period of time (one minute) across sessions.

After you enable Time Binding, configure the following time attributes:

- **Scope**—Select the scope within which the count occurs:
  - **Source.** Select this option to detect attacks from the source IP address for the specified number of times, regardless of the destination IP address.
  - **Destination.** Select this option to detect attacks to the destination IP address for the specified number of times, regardless of the source IP address.
  - **Peer.** Select this option to detect attacks between source and destination IP addresses of the sessions for the specified number of times.

- **Count**—Enter the number of times that the attack object must detect an attack within the specified Scope before the device considers the attack object to match the attack. For example, the TCP Protocol Anomaly “Segment Out of Window” is harmless and is normally seen occasionally on the network but thousands of these anomalies between given peers is suspicious.

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
<th>Default Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>rlogin</td>
<td>rlogin</td>
<td>TCP/513</td>
</tr>
<tr>
<td>rsh</td>
<td>rsh</td>
<td></td>
</tr>
<tr>
<td>rtsp</td>
<td>rtsp</td>
<td></td>
</tr>
<tr>
<td>SMB</td>
<td>Server Message Block</td>
<td></td>
</tr>
<tr>
<td>SMTP</td>
<td>Simple Mail Transfer Protocol</td>
<td>TCP/25, UDP/25</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
<td>TCP/161, UDP/161</td>
</tr>
<tr>
<td>SNMPTRAP</td>
<td>SNMP trap</td>
<td>TCP/162, UDP/162</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell</td>
<td>TCP/22, UDP/22</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer</td>
<td></td>
</tr>
<tr>
<td>syslog</td>
<td>Syslog</td>
<td>UDP/514</td>
</tr>
<tr>
<td>Telnet</td>
<td>Telnet TCP protocol</td>
<td>TCP/23, UDP/23</td>
</tr>
<tr>
<td>TFTP</td>
<td>Trivial File Transfer Protocol</td>
<td></td>
</tr>
<tr>
<td>VNC</td>
<td>Virtual Network Computing</td>
<td></td>
</tr>
<tr>
<td>Whois</td>
<td>whois</td>
<td></td>
</tr>
<tr>
<td>YMSG</td>
<td>Yahoo! Messenger</td>
<td></td>
</tr>
</tbody>
</table>
If you bind the attack object to multiple ports (see “Configuring Attack Detection Properties” on page 464), and the attack object detects that attack on different ports, each attack on each port is counted as a separate occurrence. For example, when the attack object detects that attack TCP/80 and then on TCP/8080, the count is two.

When you have completed entering the general attack properties for the attack type, click Next to configure the attack detection properties, as detailed below.

Configuring Attack Detection Properties

In the Attack Pattern screen, you can define the signature pattern of the attack, the context in which the attack occurs, and the direction and flow of the attack, as detailed below.

Configuring Attack Pattern

The attack pattern is the signature of the attack you want to detect. A signature is a pattern that always exists within an attack; if the attack is present, so is the signature. To create the attack pattern, you must first analyze the attack to detect a pattern (such as a segment of code, a URL, or a value in a packet header), then create a syntactical expression that represents that pattern. DI and IDP use a syntax based on regular expressions to match signature patterns, shown below:

Table 24: Attack Pattern Syntax

<table>
<thead>
<tr>
<th>Pattern</th>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct binary match (octal)</td>
<td>\0&lt; octal-number&gt;</td>
</tr>
<tr>
<td>Direct binary match (hexadecimal)</td>
<td>\X&lt; hexadecimal-number&gt; \X</td>
</tr>
<tr>
<td>Case insensitive matches</td>
<td>[&lt; character-set&gt;]</td>
</tr>
<tr>
<td>Match any symbol</td>
<td>.</td>
</tr>
<tr>
<td>Match 1 or more symbols</td>
<td>*</td>
</tr>
<tr>
<td>Match 0 or 1 symbols</td>
<td>?</td>
</tr>
<tr>
<td>Grouping of expressions</td>
<td>()</td>
</tr>
<tr>
<td>Alternation, typically used with ( )</td>
<td></td>
</tr>
<tr>
<td>Character range</td>
<td>[&lt; start&gt; -&lt; end&gt; ]</td>
</tr>
<tr>
<td>Negation of range</td>
<td>[^&lt; start&gt; -&lt; end&gt; ]</td>
</tr>
</tbody>
</table>

NOTE: Regular expression support is provided by the PCRE library package, which is open source software, written by Philip Hazel, and copyright by the University of Cambridge, England. The source software is available using ftp from the following web site: ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/

Some example syntax matches are shown below:
Table 25: Attack Pattern Syntax Example Matches

<table>
<thead>
<tr>
<th>This Syntax</th>
<th>Matches...</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>\x01 86 A5 00 00\x</td>
<td>the five specified bytes verbatim.</td>
<td>01 86 A5 00 00</td>
</tr>
<tr>
<td>(hello</td>
<td>world)</td>
<td>hello or world.</td>
</tr>
<tr>
<td>(hello</td>
<td>world)+</td>
<td>hello or world one or more times.</td>
</tr>
<tr>
<td>[hello]</td>
<td>hello in a case insensitive manner.</td>
<td>hElLo</td>
</tr>
<tr>
<td>[c-e]a(d</td>
<td>t)</td>
<td>Anything with the first letter of c, d, or e, the middle letter a and ending in d or t.</td>
</tr>
<tr>
<td>[^c-d]a(d</td>
<td>t)</td>
<td>Expressions that begin with a letter other than c, d, or e, have the second letter a, and end in d or t.</td>
</tr>
<tr>
<td>a*b+ c</td>
<td>Any number of “a” characters followed by one or more b characters followed by a c.</td>
<td>bc</td>
</tr>
</tbody>
</table>

To negate the pattern, enable Negate.

**Configuring Attack Context**
Select the context that defines the location of the signature.

**NOTE:** For IDP attack objects, if you selected “Any” as the Service Binding in the Attack Pattern screen, you cannot select a service context here.

If you know the service and the specific service context, select that service then select the appropriate service contexts. If you know the service, but are unsure of the specific service context, select Other then select one of the following general contexts:

**NOTE:** If you select a line, stream, stream 256, or a service context, you cannot specify IP header contents (in the Header Match screen).

- Select packet context to match the attack pattern within a packet. When you select this option, you should also specify the Service Binding (in the General tab) and define the service header options (in the Header Match tab). Although not required, specifying these additional parameters helps to improve the accuracy of the attack object, and can improve performance.
Select first packet context detect the attack in only the first packet of a stream. When the flow direction for the Attack Object is set to any, the security device checks the first packet of both the server-to-client (STC) and client-to-server (CTS) flows. If you know that the attack signature appears in the first packet of a session, choosing first packet instead of packet reduces the amount of traffic the security device needs to monitor, which improves performance.

Select stream context to reassemble packets and extract the data to search for a pattern match. However, a security device does not recognize packet boundaries for stream contexts, so data for multiple packets is combined. Select this option only when no other context option contains the attack.

Select stream 256 context to reassemble packets and search for a pattern match within the first 256 bytes of a traffic stream. When the flow direction is set to any, the security device checks the first 256 bytes of both the STC and CTS flows. If you know that the attack signature will appear in the first 256 bytes of a session, choosing stream 256 instead of stream reduces the amount of traffic that the security device must monitor and cache, improving performance.

Select line context to detect a pattern match within a specific line within your network traffic.

Configuring Attack Direction
Select the connection direction of the attack. Using single direction (instead of Any) improves performance, reduces false positives, and increases detection accuracy:

- Client to Server (detects the attack only in client-to-server traffic)
- Server to Client (detects the attack only in server-to-client traffic)
- Any (detects the attack in either direction)

Configuring Attack Flows
Select the connection flow of the attack. Using a single flow (instead of Both) improves performance and increases detection accuracy.

- Control (detects the attack in the initial connection that is established persistently to issue commands, requests, and so on.)
- Auxiliary (detects the attack in the response connection established intermittently to transfer requested data)
- Both (detects the attack in the initial and response connections)

When you have completed entering the attack detection properties for the attack type, click Next to configure the attack IP settings and protocol headers, as detailed below.
Configuring Header Match Properties

Specify specific values and options that exist within the header of the attack packet.

**NOTE:** You can configure header values only for attack objects that use a packet or first packet context. If you selected a line, stream, stream 256, or a service context (in the Detection tab) you cannot specify header contents.

If you are unsure of the options or flag settings for the malicious packet, leave all fields blank and the security device attempts to match the signature for all header contents. For each value you do enter, you must specify the relational or equality operator:

<table>
<thead>
<tr>
<th>Modifier</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>==</td>
<td>equal to</td>
</tr>
<tr>
<td>!=</td>
<td>not equal to</td>
</tr>
<tr>
<td>&gt;</td>
<td>greater than</td>
</tr>
<tr>
<td>&lt;</td>
<td>less than</td>
</tr>
</tbody>
</table>

Additionally, for each flag you must specify whether or not a flag is configured (none), the flag is set (set), or the flag is not set (unset).

**Configure IP Header Matches**

In the IP tab, for attacks that use IP and a packet context, you can set values for the following IP fields and flags:

- **Type of Service**—Specify an operand (none, =, !, >, <) and a decimal value for the service type. Common service types are:
  - 0000 Default
  - 0001 Minimize Cost
  - 0002 Maximize Reliability
  - 0003 Maximize Throughput
  - 0004 Minimize Delay
  - 0005 Maximize Security

- **Total Length**—Specify an operand (none, =, !, >, <) and a decimal value for the number of bytes in the packet, including all header fields and the data payload.

- **ID**—Specify an operand (none, =, !, >, <) and a decimal value for the unique value used by the destination system to reassemble a fragmented packet.
- **Time to Live**—Specify an operand (none, =, !, >, <) and a decimal value for the time-to-live (TTL) value of the packet. This value represents the number of routers the packet can pass through. Each router that processes the packet decrements the TTL by 1; when the TTL reaches 0, the packet is discarded.

- **Protocol**—Specify an operand (none, =, !, >, <) and a decimal value for the protocol used.

---

**NOTE:** The Protocol field does not appear for DI attack objects

- **Source**—Enter the source IP of the attacking device.

- **Destination**—Enter the destination IP of the attack target.

- **Reserved Bit**—This bit is not used.

- **More Fragments**—When set (1), this option indicates that the packet contains more fragments. When unset (0), it indicates that no more fragments remain.

- **Don’t Fragment**—When set (1), this option indicates that the packet cannot be fragmented for transmission.

### Configuring TCP Header Matches

For attacks that use TCP and a packet context, in the Protocol tab, select TCP Packet Header Fields from TCP/UDP/ICMP Header Matches menu, then set values for the following TCP fields and flags:

- **Source Port**—Specify an operand (none, =, !, >, <) and a decimal value for the port number on the attacking device.

- **Destination Port**—Specify an operand (none, =, !, >, <) and a decimal value for the port number of the attack target.

- **Sequence Number**—Specify an operand (none, =, !, >, <) and a decimal value for the sequence number of the packet. This number identifies the location of the data in relation to the entire data sequence.

- **ACK Number**—Specify an operand (none, =, !, >, <) and a decimal value for the ACK number of the packet. This number identifies the next sequence number; the ACK flag must be set to activate this field.

- **Header Length**—Specify an operand (none, =, !, >, <) and a decimal value for the number of bytes in the TCP header.

- **Data Length**—Specify an operand (none, =, !, >, <) and a decimal value for the number of bytes in the data payload. For SYN, ACK, and FIN packets, this field should be empty.

- **Window Size**—Specify an operand (none, =, !, >, <) and a decimal value for the number of bytes in the TCP window size.
- **Urgent Pointer**—Specify an operand (none, =, !, >, <) and a decimal value for the urgent pointer. The value indicates that the data in the packet is urgent; the URG flag must be set to activate this field.

- **URG**—When set, the urgent flag indicates that the packet data is urgent.

- **ACK**—When set, the acknowledgment flag acknowledges receipt of a packet.

- **PSH**—When set, the push flag indicates that the receiver should push all data in the current sequence to the destination application (identified by the port number) without waiting for the remaining packets in the sequence.

- **RST**—When set, the reset flag resets the TCP connection, discarding all packets in an existing sequence.

- **SYN**—When set, the SYN flag indicates a request for a new session.

- **FIN**—When set, the final flag indicates that the packet transfer is complete and the connection can be closed.

- **R1**—This reserved bit (1 of 2) is not used.

- **R2**—This reserved bit (2 of 2) is not used.

**UDP Headers**

For attacks that use UDP and a packet context, in the Protocol tab, select UDP Packet Header Fields from TCP/UDP/ICMP Header Matches menu, then set values for the following UDP fields:

- **Source Port**—Specify an operand (none, =, !, >, <) and a decimal value for the port number on the attacking device.

- **Destination Port**—Specify an operand (none, =, !, >, <) and a decimal value for the port number of the attack target.

- **Data Length**—Specify an operand (none, =, !, >, <) and a decimal value for the number of bytes in the data payload.

**ICMP Headers**

For attacks that use ICMP and a packet context, in the Protocol tab, select ICMP Packet Header Fields from TCP/UDP/ICMP Header Matches menu, then set values for the following ICMP fields:

- **ICMP Type**—Specify an operand (none, =, !, >, <) and a decimal value for the primary code that identifies the function of the request/reply.

- **ICMP Code**—Specify an operand (none, =, !, >, <) and a decimal value for the secondary code that identifies the function of the request/reply within a given type.

- **Sequence Number**—Specify an operand (none, =, !, >, <) and a decimal value for the sequence number of the packet. This number identifies the location of the request/reply in relation to the entire sequence.
Configuring Custom DI/IDP Attacks

ICMP ID—Specify an operand (none, =, !, >, <) and a decimal value for the identification number is a unique value used by the destination system to associate requests and replies.

Data Length—Specify an operand (none, =, !, >, <) and a decimal value for the number of bytes in the data payload.

Configuring a Protocol Anomaly Attack Object

A protocol anomaly attack object locates unknown or sophisticated attacks that violate protocol specifications (RFCs and common RFC extensions). You cannot create new protocol anomalies, but you can configure a custom attack object that controls how the security device handles a predefined protocol anomaly when detected.

NOTE: Protocol Anomaly attack objects are supported by IDP-capable security devices only, such as the ISG 2000 or ISG 1000 running ScreenOS 5.0.0-IDP1.

To configure a custom protocol anomaly attack object, you must:

- Configure the false positive setting—For details, see “Configuring Attack Detection Properties” on page 464.

- Select a predefined protocol anomaly—Select the protocol anomaly you want to use for this attack object. The list of available predefined protocol anomalies depends on the protocols supported the select target platform, as detailed in the following table:

Table 27: Supported Protocols

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Supported By</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDENT</td>
<td></td>
</tr>
<tr>
<td>IMAP</td>
<td></td>
</tr>
<tr>
<td>MSN</td>
<td></td>
</tr>
<tr>
<td>IP Packet</td>
<td></td>
</tr>
<tr>
<td>POP3</td>
<td></td>
</tr>
<tr>
<td>REXEC</td>
<td></td>
</tr>
<tr>
<td>NFS</td>
<td></td>
</tr>
<tr>
<td>SMB</td>
<td></td>
</tr>
<tr>
<td>SSH</td>
<td></td>
</tr>
<tr>
<td>HTTP</td>
<td></td>
</tr>
<tr>
<td>DHCP</td>
<td></td>
</tr>
<tr>
<td>CHARGEN</td>
<td></td>
</tr>
<tr>
<td>DISCARD</td>
<td></td>
</tr>
<tr>
<td>DNS</td>
<td></td>
</tr>
<tr>
<td>ECHO</td>
<td></td>
</tr>
<tr>
<td>LPR</td>
<td></td>
</tr>
</tbody>
</table>
Configure the time-based settings—For details, see “Configuring Time Binding” on page 463.

### Configuring a Compound Attack Object

A compound attack object combines multiple signatures and/or protocol anomalies into a single attack object, forcing traffic to match all combined signatures and/or anomalies within the compound attack object before traffic is identified as an attack. By combining and even specifying the order in which signatures or anomalies must match, you can be very specific about the events that need to take place before the security device identifies traffic as an attack.

---

**NOTE:** Compound attack objects are supported by IDP-capable security devices only, such as the ISG 2000 or ISG 1000 running ScreenOS 5.0.0-IDP1.

When configuring a custom compound attack object:

- All members of the compound attack object must use the same service setting or service binding, such as FTP, Telnet, YMSG, or TCP/80.
You can add protocol anomaly attack objects to a compound attack object.

You cannot add predefined or custom attack objects to a compound Attack Object. Instead, you specify the signature directly within the compound attack object, including such details as service (or service binding), service context, attack pattern, and direction.

You can add between 2 and 32 protocol anomaly attack objects and/or signatures as members of the compound attack object. However, all members must use the same service setting or service binding.

Configuring General Attack Properties
False positive and time-based attack properties are configured for a compound attack object the same way as they are for a signature attack object. For details, see “Configuring General Attack Properties” on page 460.

Because all members of the compound attack object must use the same service binding, the service binding you select determines the service contexts you can use for an attack pattern, as well as the available predefined protocol anomaly attack objects you can add as members.

To match all services, select Any as the Service Binding.

- When adding an attack pattern as a member, you are restricted to the contexts packet and first packet.
- When adding a predefined protocol anomaly attack object as a member, you are restricted to the IP-based protocol anomaly attack objects.

Additionally, because the number of session transactions are not known for the service, you cannot specify a scope (in the Members tab).

To match a specific service, select the service binding and provide the protocol ID, port/port range, program number if necessary.

Next, configure the members of the compound attack object, as detailed below.

Configuring Compound Attack Members
When configuring members, you add the signatures and/or protocol anomalies to detect an attack that uses multiple methods to exploit a vulnerability. The attack traffic must match all signatures and/or anomalies within the compound attack object before the device considers the traffic as an attack. To be explicit about the events in an attack, you can also specify the order in which signatures or anomalies must match before the security device identifies traffic as an attack.

Configuring Attack Object Scope
If the selected service supports multiple transactions within a single session, you can also specify whether the match should occur over a single session or can be made across multiple transactions within a session:

- Select session to allow multiple matches for the object within the same session.
Select transaction to match the object across multiple transactions that occur within the same session.

**Configuring Attack Object Ordered Match**

Use ordered match to create a compound Attack Object that must match each member signature or protocol anomaly in the order you specify. If you do not specify an ordered match, the compound Attack Object still must match all members, but the attack pattern or protocol anomalies can appear in the attack in random order.

To configure an ordered match, enable Ordered Match and use the arrow keys to reorder members.

**Configuring An Attack Pattern**

You configure the attack pattern as a member of a compound attack object as you would an attack pattern in a signature attack object. For details, see “Configuring Attack Detection Properties” on page 464.

To add an attack pattern to the compound Attack Object, click the Add icon and select Signature.

- **Pattern**—Specify the pattern to match. You construct the attack pattern just as you would when creating a new signature Attack Object. To negate the pattern, enable Negate.

- **Context**—Specify the context in which to locate the pattern. The context displays only contexts that are appropriate for the specified Service. If you selected a service binding of Any, you are restricted to the service contexts packet and first packet.

- **Direction**—Specify whether the security device should match the pattern in traffic flowing in any direction, from client to server, or from server to client.

**Adding A Predefined Protocol Anomaly Attack Object**

To add a protocol anomaly to the compound attack object, click the Add icon and select protocol anomaly. In the Attack Properties area, select an anomaly from the Key menu. The menu only displays protocol anomalies appropriate for the Service you selected.

If you selected a service binding of Any, you are restricted to the IP-based protocol anomaly attack objects.

**Configuring Direction Filter**

Use the direction filter to specify the direction (Any, Client-to-Server, Server-to-Client) of traffic in which the attack object attempts to match an attack. Each attack version in the attack object retains its own direction; however, you can use the direction filter to change which direction is monitored by the attack object. Only those attack versions that match the direction filter are active in the attack object.
By default, the direction filter is automatically set to the direction of the most recently-created or edited attack version.

Creating Custom DI Attack Groups

For DI attack objects, you can create custom attack object groups to contain your custom DI attack objects. After you add these custom groups to a DI profile, you can then configure a firewall rule to use that DI Profile.

All DI attack object groups (both predefined and custom) are considered “static” groups, meaning that they do not change. To add or delete an attack object from the group, you must manually edit the group members.

A custom attack object group can contain custom attack objects, and other custom attack object groups. You cannot add predefined attack objects or predefined attack object groups to a custom attack object group. To use both predefined and custom attack objects in a firewall rule, create a DI Profile that includes predefined and custom attack object groups, then use this profile object within the Rule Options of a firewall rule. For details on creating a DI Profile, see “Creating DI Profiles” on page 451.

NOTE: Attack group names cannot be the same as attack object names.

Creating Custom IDP Attack Groups

NetScreen-Security Manager contains a database of hundreds of predefined attack objects designed to protect networks from multiple attack vectors. For your convenience, we organize these attack objects into predefined groups.

For IDP attack objects, you can create static or dynamic groups to contain predefined or custom attack objects. A static group contains only the groups or attack objects you specify, while a dynamic group contains attack objects based on criteria you specify. Although you do not have to create a group to use an attack object within an IDP rule (you can add attack objects individually or by group), organizing attack objects into groups can help keep your Security Policies organized.

Creating Static Attack Groups

A static group contains a specific, finite set of attack objects or groups. There are two types of static groups: predefined static groups and custom static groups.

A custom static group can include the same members as a predefined static group (predefined attack objects, predefined static groups, and predefined dynamic groups), plus the following members:

- Custom attack objects
- Custom dynamic groups
- Other custom static groups
Use static groups to define a specific set of attacks to which you know your network is vulnerable, or to group custom attack objects. For example, you might want to create a group for a specific set of informational attack objects that keep you aware of what is happening on your network.

Static groups require more maintenance than dynamic groups because you must manually add or remove attack objects in a static group to change the members. However, you can include a dynamic group within a static group to automatically update some attack objects. For example, the predefined attack object group Operating System is a static group that contains four predefined static groups: BSD, Linux, Solaris, and Windows. The BSD group contains the predefined dynamic group BSD-Services-Critical, to which attack objects can be added during an attack database update.

To create a custom static group:

1. In Object Manager, select Attack Objects > IDP Objects. The IDP Objects dialog box appears.
2. Click the Custom Attack Groups tab, then click the Add icon and select Add Static Group. The New Static Group dialog box appears.
3. Enter a name and description for the static group. Select a color for the group icon.
4. To add an attack or group to the static group, select the attack or group from the Attacks/Group list and click the Add button.
5. Click OK.

For step-by-step instructions on creating a static attack object group, see the NetScreen-Security Manager Online Help topic “Adding Static Attack Groups”.

Creating Dynamic Attack Groups (IDP Only)

A dynamic group contains a dynamic set of attack objects that are automatically added or deleted based on specified criteria for the group. For example, an attack database update can add or remove attack objects from a dynamic group based on the group criteria. This eliminates the need to review each new signature to determine if you need to use it in your existing Security Policy.

A predefined or custom dynamic group can only contain attack objects and not attack groups. Dynamic group members can be either predefined or custom attack objects.

To create a custom dynamic group:

1. In Object Manager, select Attack Objects > IDP Objects. The IDP Objects dialog box appears.
2. Click the Custom Attack Groups tab, then click the Add icon and select Add Dynamic Group. The New Dynamic Group dialog box appears.
3. Enter a name and description for the static group. Select a color for the group icon.
4. In the Filters tab, click the Add icon and select one of the following:

- Add Products Filter to add attack objects based on the application that is vulnerable to the attack.
- Add Severity Filter to add attack objects based on the attack severity.

**NOTE:** All predefined attack objects are assigned a severity level by Juniper Networks. However, you can edit this setting to match the needs of your network.

- Add Category Filter to add attack objects based on category.
- Add Last Modified Filter to add attack objects based on their last modification date.

You create filters one at a time; each criteria you add is compared to the attributes for each attack object. Attack objects that do not match the criteria are immediately filtered out. If you create a filter with attributes that no attack object can match, a message appears warning you that your dynamic group has no members.

From the resulting list of matching attack objects, you can then exclude any attack objects that produce false positives on your network, or an attack object that detects an attack to which your network is not vulnerable.

**NOTE:** A dynamic group cannot contain another group, (predefined, static, or dynamic). However, you can include a dynamic group as a member of a static group.

**EXAMPLE: CREATING A DYNAMIC GROUP**

To create a dynamic group:

1. In the Custom Attack Groups tab, click the Add icon and select Add Dynamic Group. The New Dynamic Group dialog box appears.

2. Enter a name and description for the group. Select a color for the group icon.

   **Figure 104: New Dynamic Group**

<table>
<thead>
<tr>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
</tr>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Color</td>
</tr>
<tr>
<td>Description</td>
</tr>
</tbody>
</table>

3. In the Filters tab, click the Add icon and add the filters that determine which attack objects should be in the group:

   a. Add a Products filter to add attack objects that detect attacks against all Microsoft Windows operating systems.
b. Add a Severity filter to add attack objects that have a severity level of critical or major.

IDP automatically applies all filters to the entire attack object database, identifies the attack objects that meet the defined criteria, and adds the matching objects as members of the group.

4. View the members of the group by clicking the Members tab:

Figure 105: New Dynamic Group Members

<table>
<thead>
<tr>
<th>Filters</th>
<th>Members</th>
</tr>
</thead>
<tbody>
<tr>
<td>CUPS Jobs Form Exploit</td>
<td></td>
</tr>
<tr>
<td>CVS Entry Line Tag Heap Overflow</td>
<td>(predefined)</td>
</tr>
<tr>
<td>Kadmin for krb-4.1.2 Buffer Overflow</td>
<td>(predefined)</td>
</tr>
<tr>
<td>Linux rsync recv_exclude_list Buffer Overflow</td>
<td>(predefined)</td>
</tr>
<tr>
<td>Samba Trans2Rool Buffer Overflow</td>
<td>(predefined)</td>
</tr>
<tr>
<td>Malformed Packet Exploit</td>
<td>(predefined)</td>
</tr>
<tr>
<td>APP: Troltech Gt BMP Handling Overflow</td>
<td>(predefined)</td>
</tr>
<tr>
<td>ISC dhcpd DHCP_HOST Format String</td>
<td>(predefined)</td>
</tr>
<tr>
<td>ISC DHCPv3 Format String Exploit</td>
<td>(predefined)</td>
</tr>
<tr>
<td>VMu-ftpd realpath() Buffer Overflow</td>
<td>(predefined)</td>
</tr>
<tr>
<td>VMu-ftpd realpath() Buffer Overflow</td>
<td>(predefined)</td>
</tr>
<tr>
<td>Apache &quot;Transfer-Encoding: chunked&quot; Worm Infection Attempt</td>
<td>(predefined)</td>
</tr>
<tr>
<td>Apache: apache knowledgeable Attack</td>
<td>(predefined)</td>
</tr>
</tbody>
</table>

5. Click OK to save the dynamic group.

Updating Dynamic Groups

When you are satisfied with the group criteria and its members, use the group in a Security Policy. The next time you update your attack objects, the update automatically performs the following:

- For all new attack objects, compares the predefined attributes of each attack object to each dynamic group criteria and adds the attack objects that match.

- For all updated attack objects, removes attack objects that no longer meet their dynamic group criteria. The update also reviews updated attack objects to determine if they now meet any other dynamic group criteria, and adds them to those groups if necessary.

- For all deleted attack objects, removes the attack objects from their dynamic groups.
You can also edit a dynamic group manually, adding new filters or adjusting existing filters to get exactly the type of attack objects you want.

---

**NOTE:** You can edit a custom dynamic attack group from within an IDP rule in a Security Policy. Double-click the group icon in the Attack Objects column of an IDP rule to display the Dynamic Group dialog box, make the desired changes, then click OK to save your edits.

---

**Editing a Custom Attack Group**

To modify a custom attack group, double-click the group in the Custom Attack Groups tab in the IDP Objects dialog box. The Static Group or Dynamic Group dialog box appears, with the previously-configured information displayed. Enter any changes you want to make and then click Apply to continue making changes or click OK to close the dialog box.

**Deleting a Custom Attack Group**

To delete a custom attack group, right-click the group in the Custom Attack Groups tab in the IDP Objects dialog box, and then select Delete. A confirmation window asks you to verify that you want to delete the item. Click OK.

---

### Configuring AntiVirus Objects

Security devices provide two antivirus scanning methods:

- **External AV scanning**—This method uses a Trend Micro device for scanning. (This option is not supported by devices running ScreenOS 5.1 or higher.) The security device forwards all traffic to be scanned to the Trend Micro device. To configure external AV scanning, use the AV Scanner settings (detailed below).

- **Internal AV scanning**—This method uses the AV scanner on the security device, and is not supported by all security devices. Internal scanning may be configured on a per-device basis, or it may be configured via templates. This section describes how to create the templates. Only available on the 5GT and HSC devices.

### Configuring External AV Profiles

External AV profiles define the external AV scanner server that a security device uses to detect viruses in specific protocols. You must configure an AV profile when using external AV for virus protection on your security device. After you have configured an AV profile, you can use the profile within a firewall rule.

**NOTE:** You can configure additional settings for external antivirus protection on the security device itself. For details, see “Configuring External AV Scanners” on page 316.

External AV profiles contain the following information:
Server Name and Port—You must specify the IP address and port number of the external antivirus server that contains your virus definitions.

Protocols and Timeouts—You must specify the protocols (HTTP and/or SMTP) that the external AV server scans for viruses. The default protocol timeout is 180 seconds, but you can edit this default to meet your networking requirements.

You must use the AV profile in a firewall rule and install that rule on a security device before the external scanner can begin inspecting traffic for viruses. For details on using AV profiles in rules, see “Configuring AntiVirus For Firewall Rules” on page 551.

**EXAMPLE: CONFIGURING AN EXTERNAL AV PROFILE**

In this example, you configure an AV profile that sends all HTTP traffic to an external TrendMicro antivirus server at 1.2.2.20 for virus checking. Because you anticipate heavy HTTP loads on the network, you increase the timeout from 180 seconds (the default setting) to 300 seconds.

1. In the main navigation tree, select Object Manager > AV Objects > External.
2. In the main display area, click the Add icon. The New AntiVirus Profile dialog box appears.
3. Configure the following:
   - For Name, scanner1_HTTP
   - For Server Name, enter 1.2.2.20.
   - For Server Port, leave the default port number of 3300.
4. Select HTTP, then configure the timeout as 300 seconds.
5. Click OK to save the new profile.

**Configuring Internal AV Profiles**

Internal AV profiles allow you to set AV settings for multiple devices via a policy. NetScreen-Security Manager comes with a predefined AV profile, or you can create your own.

**View the Predefined Profile**

To view the predefined AV profile, open Object Manager > AV Objects > Internal > Predefined Profiles. Select the predefined profile, then click the edit button. You cannot make changes to the profile.

**Create Custom AV Profiles**

To create a custom AV profile, open Object Manager > AV Objects > Internal > Custom Profiles. Click the Add button.

Populate the fields of the New Internal Antivirus Profile dialog:
General information—Assign a name and color to the profile, and enter a comment describing the purpose of the profile.

For each protocol type, check the Enable checkbox to enable scanning for that protocol, then set the following settings for each enabled protocol:

- the Scan Mode: All, Intelligent, or by File Extension. If you select Scan by File Extension, you must populate the Ext List Include field.
- Scanning Timeout: scans that take longer than this time out and are not completed.
- Decompress Layer: the number of levels of decompression to uncompress before scanning. A decompression setting of 2 would all the scanning of a .zip file within a .zip file.
- Skip Mime (HTTP only): if checked, causes the scanner to skip any mime types listed in the Mime List field.
- Ext List Include: a list of file extensions to examine for viruses. Extension lists are created under Object Manager > AV Objects > Extension Lists.
- Ext List Exclude: a list of file extensions to not examine for viruses. Extension lists are created under Object Manager > AV Objects > Extension Lists.
- Mime List (HTTP only): the list of mime types to not scan. Netscreen-Security Manager ships with a default mime type list, or you can create your own under Object Manager > AV Objects > Custom Mime Lists.
- Email Notify Virus Sender (IMAP, POP3, SMTP only): Notifies an email sender if a virus was found in the email.
- Email Notify Scan-Error Sender (IMAP, POP3, SMTP only): Notifies an email sender if the email was dropped due to a scan error.
- Email Notify Scan-Error Recipient (IMAP, POP3, SMTP only): Notifies an email recipient if the email was passed due to a scan error.

Configuring Extension Lists
You can configure AV profiles to scan (or not scan) files based on their file extension. File extension include lists and exclude lists are the same kind of lists. They become include or exclude lists depending on how they are added to a profile.

To create a file extension list object, open Object Manager > AV Objects > Internal > Extension lists. Click the Add button.

Populate the following fields in the New Internal Antivirus Ext List dialog:

- Name: Give the extension list a descriptive name.
- Color: Assign a color, if desired.
Configuring Web Filtering Objects

Web Filtering (Integrated) enables you to create a Web Filtering profile for all of your security devices by binding the profile to the firewall rule. With a Web Filtering profile, the security device intercepts each HTTP request and determines whether to permit or block access to a requested website by categorizing the URL and matching the URL category to the Web Filtering profile. You can then bind the Web Filtering profile to the firewall rule.

To configure a security device for Web Filtering, you need to:

- Obtain a license key to enable the Web Filtering option on security devices. For details, see “Managing License Keys” on page 414.
- Configure at least one Domain Name Server (DNS) so the security device can resolve the SurfControl CPA server name to an address.
- Configure Web Filtering on the security device. For details, see “Configuring Web Filtering” on page 322.

URL Categories

A URL category is a list of URLs organized by content. There are two types of categories: Custom Lists and Predefined Categories.
Custom Lists

You can group URLs and create custom lists specific to your needs. You can include up to 20 URLs in each list. When you create a list, you can add either the URL or the IP address of a website. When you add a URL to a custom list, the security device performs a Domain Name Server (DNS) lookup, resolves the hostname into IP addresses and caches this information.

When a user tries to access a website by typing the IP address of the website, the security device checks the cached list of addresses and tries to resolve the hostname. It is important to enter both the URL and the IP address(es) of a website.

**NOTE:** When a URL exists in both a custom list and a predefined category, the security device matches the URL to the custom list first.

**EXAMPLE:** CREATING A URL CUSTOM LIST

In this example you create a custom list called Competitors, Gaming.

1. In the main navigation tree, select Object Manager > Web Filtering (Integrated) > URL Categories > Custom Lists.

2. Click the Add icon. The New URL Categories dialog box appears.

3. For Name, enter Competitors, Gaming.

4. Click the Add icon. The New URL Entries dialog box appears. Configure as shown below, then repeat to add a second URL Entry:
For the first URL entry, enter www.games1.com then click OK.

For the second URL entry, enter www.games2.com then click OK.

5. Click OK to save the new Custom List.

Predefined Categories

The security devices can use the predefined SurfControl URL categories to determine the category of a URL. SurfControl Content Portal Authority (CPA) servers maintain a large database of web content classified into approximately 40 categories.

To view the predefined SurfControl URL categories, select Web Filtering (Integrated) > URL Categories > Predefined Categories.
URL Profiles

A Web Filtering profile consists of a group of URL categories and their corresponding actions. NetScreen-Security Manager supports two types of profiles: Custom and Predefined.

Custom Profiles

When you create a custom Web Filtering profile, you can add both custom and SurfControl predefined URL categories to the profile, then specify a category for the Black List and/or the White List.

- Black List—The security device always blocks access to the web sites in the Black List. You can create a custom category for the Black List or use a predefined category.

- White List—The security device always allows access to the web sites in the White List. You can create a custom category for the White List or use a predefined category.

You can also configure the default action for the profile:

- Permit—The security device allows access to the website.

- Block—The security device does not allow access to the website. When the device blocks access to a website, it displays a message indicating the category of the URL.

EXAMPLE: CREATING A WEB FILTERING CUSTOM PROFILE

In this example, you create a custom profile called Competitors.

1. From the main navigation tree, select Object Manager > Web Filtering (Integrated) > URL Profiles > Custom Profiles.

2. Click the Add icon. The New URL Profile dialog box appears. Configure the following, then click OK:

   - For Name, enter Competitors.
   - For Comments, enter All Competitors.
   - For Black List, select Competitors, Gaming.
   - For White List, select None.

3. In Main Categories, click the Add icon and select the following URL categories: Art and Entertainment, Games. Click OK to add to the profile object.

4. Select Games, then click the Edit icon. Change the default action for the Games category to Block, then click OK, as shown below:
5. For Action for all Other URLs, leave the default setting (Block).

6. Click OK to save the new Profile.

Predefined Profiles

NetScreen-Security Manager provides a default profile called **ns-profile**. It lists the SurfControl predefined URL categories and their corresponding actions.

**NOTE:** If the URL in an HTTP request is not listed in a custom profile, then the security device defaults to ns-profile.

You cannot edit the default profile or add a Black List or White List to it.

**EXAMPLE:** VIEWING THE PREDEFINED PROFILE

To view the predefined profile:

1. In the main navigation tree, select Object Manager > Web Filtering (Integrated) > URL Profiles > Predefined Profiles.

2. Double-click ns-profile. The URL Profile dialog box displays the Categories and Actions for the ns-profile.

**NOTE:** You cannot change the list of predefined categories in ns-profile.
Configuring GTP Objects

To enable a security device to manage GTP traffic, you must create a GTP Object and then apply it to a Security Policy rule. The rule with the GTP object defines how the device handles GTP packets: If a GTP packet matches the rule, the device attempts to further match the packet data with the parameters set in the GTP object.

Using GTP objects, you can configure multiple rules that enforce different GTP configurations in the same Security Policy. For example, you can configure a Security Policy that enables a device to control GTP traffic differently based on source and destination zones and addresses, action, and so on.

You configure GTP Objects in the Object Manager. From the main navigation tree, select Object Manager > GTP Objects, then click the Add icon to display the New GTP Object configuration screens. For each object, you can configure the following settings:

- Configuring Info
- Configuring Traffic Logging and Counting
- Configuring IMSI Prefix and APN Filtering
- Configuring GTP Message Filtering
- Configuring Subscriber Tracing (Lawful Interception)

The following sections detail each GTP setting. For an example on creating a GTP object, see “Creating a GTP Object” on page 491.

Configuring Info

The Info settings define the basic properties of the GTP object, and specify how the security device should handle GTP messages and tunnels.

Limiting GTP Message Length

To limit the length of a GTP message, you can specify the minimum and maximum number of bytes permitted in a message length field. In the GTP header, the message length field indicates the length of the GTP payload. It does not include the length of the GTP header itself, the UDP header, or the IP header.

The default minimum and maximum GTP message lengths are 0 and 65535, respectively.

Limiting GTP Message Rate

To limit the rate of network traffic from a security device to a GPRS Support Node (GSN), you can specify the number of packets per second permitted for GTP-Control (GTP-C) messages.

Because GTP-C messages require processing and replying, they can overwhelm a GSN. Setting a rate limit on GTP-C messages can protect your GSNs from Denial-of-Service (DoS) attacks such as:
Border Gateway bandwidth saturation—A malicious operator connected to the same GRX as your PLMN can generate enough network traffic directed at your Border Gateway, so that legitimate traffic is starved for bandwidth in or out of your PLMN, thus denying roaming access to or from your network.

GTP flood—GTP traffic can flood a GSN, forcing it to spend its CPU cycles processing illegitimate data. This can prevent subscribers from roaming, forwarding data to external networks, or prevent a GPRS attach to the network.

To limit the GTP message rate, enable Limit (packets/second) and enter the maximum number of packets per second that a security device can send to a GSN (the default is unlimited).

Limiting GTP Tunnels
GSNs use GTP tunnels to transmit GTP traffic using the GPRS Tunneling Protocol (GTP). Because GSNs have a limited capacity for GTP tunnels, you might want to configure the security device to limit the number of GTP tunnels created.

To limit GTP tunnels, enable Limit (tunnels/GSN) and enter the maximum number of tunnels permitted for each GSN (the default is unlimited).

Removing Inactive GTP Tunnels
To configure a security device to detect and remove inactive GTP tunnels automatically, configure the GTP Tunnel Inactivity Timeout (hours). A GTP tunnel might hang (become inactive) when a “delete pdp context response” message gets lost on a network, or a GSN does not properly shut down.

The security device automatically removes a GTP tunnel that is idle for the specified timeout value. The default timeout value is 24 hours.

Validating Sequence Numbers
When using a security device between the GGSNs, you can configure the device to validate sequence numbers for the GGSN and drop out-of-sequence packets. This helps conserve GGSN resources by preventing the unnecessary processing of invalid packets.

The header of a GTP packet contains a Sequence Number field, which indicates the order of the packets arriving at the GGSN. During the PDP context activation stage:

- The sending GGSN uses zero (0) as the Sequence Number value for the first G-PDU it sends through a tunnel to another GGSN. The sending GGSN then increments the Sequence Number value for each following G-PDU it sends. The value resets to zero when it reaches 65535.

- The receiving GGSN sets its counter to zero. When it receives a valid G-PDU, it increments its counter by one. The counter resets to zero when it reaches 65535. The receiving GGSN compares the Sequence Number in the arriving packet with the sequence number in its counter. If the numbers correspond, the GGSN forwards the packet; if they differ, the GGSN drops the packet.

To enable the device to validate sequence numbers for the GGSN, enable Sequence Number Validation. By default, validation is disabled.
Filtering GTP-in-GTP Packets
To enable a security device to detect and drop a GTP packet that contains another GTP packet in its message body, enable GTP in GTP Denied.

Configuring Traffic Logging and Counting
When you enable traffic logging and counting for a GTP object, the security device generates log entries for deleted GTP tunnels and GTP traffic events.

Traffic Counting
A security device can count the number of user data and control messages (or bytes of data), received from and forwarded to the GGSNs and SGSNs that the device protects. The device counts traffic for each GTP tunnel separately, and differentiates GTP-User and GTP-Control messages.

To enable counting, select Count By Message or Count By Byte. When counting is enabled and tunnel is deleted, the device counts and logs the total number of messages or bytes of data that it received from and forwarded to the SGSN or GGSN.

To view log entries for deleted GTP tunnels, use the Log Viewer. For details on the information provided in the GTP log entry, see “GTP Log Entries” on page 901.

Traffic Logging
A security device creates log entries for GTP events based on the status of the GTP packet. For each event type, you can also specify how much information (basic or extended) you want about each packet (for details, see “GTP Log Entries” on page 901).

To configure GTP logging, select basic or extended for each GTP packet status:

- Log Forwarded Packets—When enabled, the device creates a log entry for each GTP packet that was transmitted because it was permitted by the Security Policy.

- Log Dropped Packet Due to Type/Length/Version—When enabled, the device creates a log entry for each GTP packet that was dropped because it was denied by the Security Policy.

- Log Dropped Packet Due to Invalid State—When enabled, the device creates a log entry for each GTP packet that was dropped because it failed stateful inspection.

- Log Dropped Packet Due to GSN Tunnel Limit—When enabled, the device creates a log entry for each GTP packet that was dropped because the maximum limit of GTP tunnels for the destination GSN was reached.

- Log Dropped Packet Due to GSN Rate Limit—When enabled, the device creates a log entry for each GTP packet that was dropped because the maximum rate limit of the destination GSN was reached.
You can also specify the frequency that a security device creates log entries for rate-limited messages. Setting a logging frequency conserves resources on the syslog server and security device, and can avoid a logging overflow of messages. By default, the frequency is 2, meaning the security device creates a log entry for every two messages above the set rate limit.

To view GTP traffic log entries, use the Log Viewer.

**Configuring IMSI Prefix and APN Filtering**

You can use the IMSI Prefix and APN to restrict access to a specific set of mobile subscribers.

**Creating an APN Filter**

An Access Point Name (APN) is included in the header of a GTP packet, and provides information on how to reach a network. By default, a security device permits all APNs. However, you can configure the device to filter APNs, enabling access only for those APNs you specify, and restricting roaming subscribers’ access to external networks.

You can specify up to 2000 permitted APNs. When APN filtering is enabled, it applies only to “create pdp request” messages. For these messages to pass an APN filter, the GTP packet must match both the APN name filter and the Selection Mode filter:

- **APN Domain Name filter**—The device attempts to match the APN in a GTP packet to the APNs set in the GTP object. If the two APNs match, the device passes the packet to the selection mode filter.

- **Selection Mode Filter**—The device attempts to match the Selection Mode for the GTP packet and the GTP object. If the two modes match, the device forwards the GTP packet; if the modes do not match, the device drops the GTP packet.

Additionally, you can filter GTP packets based on the combination of an IMSI prefix and an APN. For details, see “Creating an IMSI Prefix Filter” on page 490.

**Setting the Network ID (APN Domain Name)**

To set an APN filter, you need to know the network ID, which identifies the name of an external network.

---

**NOTE:** Because the APN domain name (network ID) can potentially be very long and contain many characters, you can use the wildcard “*” as the first character of the APN to indicate that the APN also includes all preceding characters. However, because APN filtering is based on perfect matches, using the wildcard “*” can prevent the inadvertent exclusion of APNs that you would otherwise authorize.

---

**Setting a Selection Mode**

You must also set a Selection Mode, which indicates the origin of the APN and if the user subscription has been verified by the Home Location Register (HLR). You can set one of the following Selection Modes:
- Mobile Station—MS-provided APN, subscription not verified. This Selection Mode indicates that the mobile station (MS) provided the APN and that the HLR did not verify the user's subscription to the network.

- Network—Network-provided APN, subscription not verified. This Selection Mode indicates that the network provided a default APN because the MS did not specify one, and that the HLR did not verify the user's subscription to the network.

- Verified—MS or Network-provided APN, subscription verified. This Selection Mode indicates that the MS or the network provided the APN and that the HLR verified the user's subscription to the network.

Creating an IMSI Prefix Filter

A GSN (GPRS Support Node) identifies a mobile station by its IMSI (International Mobile Station Identity). An IMSI is composed of three elements:

- The MCC (Mobile Country Code)
- The MNC (Mobile Network Code)
- The MSIN (Mobile Subscriber Identification Number)

The MCC and MNC combine to create the IMSI prefix, which identifies the mobile subscriber's home network (PLMN). By default, a security device does not perform IMSI prefix filtering on GTP packets. You can use the IMSI prefix to configure a security device to deny GTP traffic sent from non-roaming partners.

When you set an IMSI prefix in the GTP object, the security device filters “create pdp request” messages and permits only GTP packets with a matching IMSI prefix. If the prefix does not match, the security device drops the GTP packet. You can set up to 1000 IMSI prefixes for each device (one per each filter).

To disable IMSI prefix filtering, remove all MCC-MNC pairs from the GTP object.

Configuring GTP Message Filtering

By default, the security device permits all GTP message types. You can configure a security device to filter GTP packets and drop them based on their message type.

A GTP message type includes one or many messages. When you drop a message type, you automatically drop all messages of the specified type. For example, if you select to drop the sgsn-context message type, you also drop “sgsn context request”, “sgsn context response”, and “sgsn context acknowledge” messages.

You drop message types based on the GTP version number, enabling you to drop message types for one version and permit them for another version.

Configuring Subscriber Tracing (Lawful Interception)

You can configure a security device to identify subscribers based on IMSI prefixes or Mobile Station-Integrated Services Data Network (MS-ISDN) identification, then log the contents of their GTP-User Data (GTP-U) or GTP-Control (GTP-C) messages.
To enable subscriber tracing, you must configure the following:

- **Set Subscribers**—Set the number of subscribers that the security device actively traces concurrently. The default number of simultaneous active traces is three (3).

- **Specify Log Bytes**—Specify the number of bytes of data to log for a GTP-U packet. The default value is zero, meaning that the device does not log any content from a GTP-U packet. When you enter a number other than zero, the security device sends the logged packets to an external server (such as Syslog) dedicated to Lawful Interception operations.

- **Set ID**—For each subscriber you want to trace, enter their ID number and select Based on IMSI or Based on MSISDN.

**EXAMPLE: CREATING A GTP OBJECT**

1. In Object Manager, select GTP Objects, then click the Add icon in the main display area. The New GTP Object dialog box appears.

2. In the Info tab, configure the following settings:
   - For Name, enter GPRS1, then enter a color and comment for the object.
   - Select Sequence Number Validation.
   - Select GTP in GTP Denied.
   - Leave all other defaults.

3. In the GTP navigation tree, select Traffic Logging/Counting. Configure the following:
   - For Traffic Counters, select Count by Message.
   - Select Basic for the following message types: Log Forwarded Packets, Log Dropped Packet Due to Type/Length/Version, and Log Dropped Packet Due to Invalid State.
   - Leave all other defaults.

4. In the GTP navigation tree, select IMSI Prefix and APN Filtering. Click the Add icon to display a new IMSI Prefix and APN Filter Entry dialog box. Configure the following, then click OK:
   - For APN, enter mobiphone.com.mnc123.mcc456.gprs.
   - Select MCC-MNC and enter the code 24656.
   - For Selection Mode, select Mobile Station, Network, and Verified.

5. In the GTP navigation tree, select Subscriber Tracing.
   - For Maximum Number of Simultaneous Active Traces, enter 2.
   - For Number of Bytes to Be Saved to Log, enter 1020.
6. Click the Add icon to display a New Subscriber ID dialog box. Configure the following, then click OK:
   - For ID, enter 345678.
   - For ID Type, select Based on IMSI.

7. Click OK to save the new Subscriber ID, then click OK to save the GPRS1 object.

Configuring Service Objects

Service objects represent the IP traffic types for existing protocol standards. Security devices monitor and manage network traffic using these protocols. NetScreen-Security Manager includes predefined service objects for most standard services. You can also create custom service objects to represent services that are not included in the list of predefined service objects, or to represent a custom service running on your network.

You use service objects to create protected resources and specify the type of service within a Security Policy:

- In a protected resource, select a service or group of services to define the types of traffic you are permitting to and from the resource.
- In individual rules within a firewall or IDP rulebase, select one or more services or groups of services to define the types of IP traffic to which the rule applies. The action of the rule applies when the security device detects packets that use the specified service type.

Viewing Predefined Services

You can view predefined services in a tree or table format. The Service Tree displays services in a tree format, with service groups and individual services. The Service Table displays services in a table format, and includes the following details:

<table>
<thead>
<tr>
<th>Table 28: Service Table Tab Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Type</td>
</tr>
<tr>
<td>Timeout</td>
</tr>
<tr>
<td>Category</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Non-ICMP Src Port</td>
</tr>
</tbody>
</table>
Chapter 8: Configuring Objects

To view service object properties, double-click a service object. In addition to the service name, category, and service timeout value, you can view the following service settings:

- For Non-ICMP services, the service object displays the protocol ID, source port range, and destination port range.
- For ICMP services, the General tab displays the Internet Control Message Protocol (ICMP) type and code.
- For Sun-RPC services, the Sun-RPC tab displays the Sun Microsystems program identifiers. Sun Remote Procedure Call (Sun-RPC), also known as Open Network Computing (ONC) RPC, enables a program running on one host to call procedures in a program running on another host. Because of the large number of RPC services and the need to broadcast, the transport address of an RPC service is dynamically negotiated based on the service's program number and version number. Several binding protocols are defined for mapping the RPC program number and version number to a transport address.

---

**NOTE:** The transport address is comprised of the port number of the server, the program ID, and the version number.

---

NetScreen-Security Manager and security devices support 13 Sun-RPC predefined services. To permit or deny all Sun-RPC requests, include the Sun-RPC-Any service in a firewall or IDP rule; to permit or deny a Sun-RPC request by specific program number, include that service (or create a custom service) in the rule.

- For MS-RPC services, the MS-RPC tab displays the Microsoft universal unique identifiers (UUIDs). Microsoft Remote Procedure Call (MS-RPC) is the Microsoft implementation of the Distributed Computing Environment (DCE) RPC. Like the Sun-RPC, MS-RPC enables a program running on one host to call procedures in a program running on another host. Because of the large number of RPC services and the need to broadcast, the transport address of an RPC service is dynamically negotiated based on the service program's Universal Unique IDentifier (UUID).

NetScreen-Security Manager and security devices support 27 MS-RPC predefined services and 3 MS-RPC predefined service groups. To permit or deny all MS-RPC requests, include the MS-RPC-Any service in a firewall or IDP rule; to permit or deny an MS-RPC request by specific UUID, include that service (or create a custom service) in the rule.

You can view details for a predefined service object, but you cannot edit that service object.
Configuring Custom Services

You can create custom service objects to represent protocols that are not included in the predefined services or to meet the unique needs of your network.

NOTE: Sun-RPC protocols and regular TCP/UDP/ICMP protocols cannot be in the same service object. MS-RPC protocols and regular TCP/UDP/ICMP protocols cannot be in the same service object.

To add a service object, in the Object Manager, select Service Objects > Custom Service Objects. In the main display area, click the Add icon and select Service to display the New Service dialog box. Configure the following parameters:

- **Name**—Enter a name for the service.
- **Timeout**—Select the session timeout after which an inactive session is removed.
  - **Never**—The session does not timeout.
  - **Default**—Use the default timeout for the selected protocol. The default timeout for TCP connections is 30 minutes. The default timeout for UDP connections is 1 minute.
  - **User-defined**—Enter a session timeout value. The maximum timeout value for TCP and UDP connections is 2160 minutes.
- **Color**—Select a color to represent this service object in the NetScreen-Security Manager UI.
- **Comment**—Add a comment, if desired.
- **Add the service entry**:
  - For ICMP services, in the General tab click the Add icon. Enter the ICMP type and code, then click OK. For details on ICMP type, see the NetScreen-Security Manager Online Help.
  - For Sun-RPC services, select the Sun-RPC tab, then click the Add icon. Enter high and low program identifiers, then click OK. You can add up to eight program ranges; ensure that the Program High value is greater than or equal to the Program Low value.
  - For MS-RPC services, select the MS-RPC tab, then click the Add icon. Enter a UUID, then click OK. A UUID is 36 characters.
  - For other non-ICMP services, in the NON-ICMP Service Entries area, click the Add icon. Select the protocol type and configure the source and destination ports, the click OK. To create a service object that uses multiple ports for the same service, add two service entries with different ports.

NOTE: For the complete list of the Sun Microsystems Program IDs and Microsoft UUIDs, refer to the Juniper Networks ScreenOS online help.
Service Object Groups

You can group services together as a service object group, then use that group in Security Policies and VPNs to simplify administration. Each service object can be referenced by multiple service object groups. Service object groups can contain both predefined and custom service objects, as well as other service object groups.

To add a service object group:

1. In the navigation tree, select Object Manager > Service Objects.
2. In the main display area, click the Add icon and select New > Group. The new Service Group dialog box appears.
3. Enter a name, color, and comment for the service object group.
4. In the Non-members area, select the service objects or service object groups you want to add to the group (hold CTRL to select multiple objects), then click Add.
5. Click OK.

The new service object group appears in the Service Tree and Service Table tabs.

EXAMPLE: CREATING A CUSTOM SERVICE AND GROUP

In this example, you create a custom service object to represent the Ident service and a custom service group that includes this service.

To create the custom Ident service:

1. In the main navigation tree, select Object Manager > Service Objects > Custom Service Objects.
2. In the main display area, click the Add icon and select Service. The New Service dialog box appears.
3. Configure the following:
   a. For Name, enter Ident
   b. For Timeout, select Default.
   c. For Color, select blue.
   d. Enter a Comment, if desired.
4. In the Non-ICMP Services Entries area, click the Add icon and select TCP. The New Service Entry dialog box appears. Configure the following:
   a. For Source Port, select Range.
   b. For Source Port Range, enter 0 to 65535.

NOTE: Service object group names cannot be the same as service object names.
c. For Destination Port, select Specific.
d. For Specific Port, enter 113.

5. Click OK to save the new service entry, then click OK again to save the new service object.

6. In the main display area, click the Add icon and select Group. The New Service Group dialog box appears. Configure the following:
   a. For Name, enter Remote Mail.
   b. For Color, select pink.
   c. Enter a Comment, if desired.
   d. In the non-members area, select the following services (press and hold Ctl to select multiple services):
      - FTP
      - HTTP
      - Ident
      - MAIL
      - POP3
      - TELNET
   e. Click Add to add the services as members of the group, then click OK to save the new service group.

EXAMPLE: CREATING A CUSTOM SUN-RPC SERVICE
In this example, you create a service object called my-sunrpc-nfs to use the Sun RPC Network File System, which is identified by two Program IDs: 100003 and 100227. Because Sun RPC services use dynamically negotiated ports, you cannot use regular service objects based on fixed TCP/UDP ports to permit them in security policy. Instead, you must create sun rpc service objects using program numbers. For example, NFS uses two program numbers: 100003 and 100227. The corresponding TCP/UDP ports are dynamic. To permit the program numbers, you create a sun-rpc-nfs service object that contains these two numbers. The ALG maps the program numbers into dynamically negotiated TCP/UDP ports, and permits or denies the service based on a policy you configure.

To create the Sun-RPC service:

1. In the main navigation tree, select Object Manager > Service Objects > Custom Service Objects.

2. In the main display area, click the Add icon and select Service. The New Service dialog box appears.

3. Configure the following:
Configuring Service Objects

Chapter 8: Configuring Objects

4. Select the Sun-RPC tab.
   a. Configure the first service entry. Click the Add icon to display the New Service Entry dialog box, configure the following, then click OK:
      - For Program Low, enter 100003.
      - For Program High, enter 100003.
   b. Configure the second service entry. Click the Add icon to display the New Service Entry dialog box, configure the following, then click OK:
      - For Program Low, enter 100227.
      - For Program High, enter 100227.

5. Click OK again to save the new service object.

EXAMPLE: CREATING A CUSTOM MS-RPC SERVICE
In this example, you create a service object called my-ex-info-store that includes the UUIDs for the MS Exchange Info Store service. Because MS RPC services use dynamically negotiated ports, you cannot use regular service objects based on fixed TCP/UDP ports to permit them in a security policy. Instead, you must create MS RPC service objects using UUIDs. The MS Exchange Info Store service, for example, uses the following four UUIDs:

- 0e4a0156-dd5d-11d2-8c2f-00c04fb6bcde
- 1453c42c-0fa6-11d2-a910-00c04f990f3b
- 10f24e8e-0fa6-11d2-a910-00c04f990f3b
- 1544f5e0-613c-11d1-93df-00c04fd7bd09

The corresponding TCP/UDP ports are dynamic. To permit them, you create an ms-exchange-info-store service object that contains these four UUIDs. The ALG maps the program numbers into dynamically negotiated TCP/UDP ports based on these four UUIDs, and permits or denies the service based on a rule you configure.

To create the MS-RPC service:

1. In the main navigation tree, select Object Manager > Service Objects > Custom Service Objects.

2. In the main display area, click the Add icon and select Service. The New Service dialog box appears.
3. Configure the following:
   a. For Name, enter my-ex-info-store
   b. For Timeout, select Default.
   c. For Color, select blue.
   d. Enter a Comment, if desired.

4. Select the MS-RPC tab. Configure a service entry for each of the following UUIDs:
   - 0e4a0156-dd5d-11d2-8c2f-00c04fb6bcde
   - 1453c42c-0fa6-11d2-a910-00c04f990f3b
   - 10f24e8e-0fa6-11d2-a910-00c04f990f3b
   - 1544f5e0-613c-11d1-93df-00c04fd7bd09

5. Click OK to save the new service object.

Configuring Authentication Servers

An authentication server provides authentication for NetScreen-Security Manager administrators and remote access services (RAS) users on your network. When the security device receives a connection request that requires authentication verification, the device requests an authentication check from the external auth server specified in the policy, L2TP tunnel configuration, or IKE gateway configuration. The device then acts as a relay between the user requesting authentication and the auth server granting authentication.

In NetScreen-Security Manager, an auth server is an object used in Security Policies, IKE gateways, and L2TP tunnels. Each security device includes a default authentication server; however, to enable an external RADIUS, SecureID, or LDAP server to provide authentication, you must configure an external authentication server object. You can also configure a RADIUS authentication server object to provide authentication for the global domain and each subdomain. For details on configuring a RADIUS server, see “Configuring a RADIUS Authentication Server” on page 501.

NOTE: You must also define routes that direct authentication requests to the RADIUS, SecureID, and LDAP servers.

To configure general authentication server object properties, in the main navigation tree, select Object Manager > Authentication Servers then click the Add icon. The General, Redundancy, and Identity tabs are the same for all server types; in the Server Type tab, select the authentication server type (RADIUS, SecureID, LDAP) to configure specific settings for that server type.
Configuring General Authentication Server Settings

In the General tab, configure a name, color, and comment that uniquely identify the object, then specify the IP address of the main authentication server; this is the IP address of the server that handles authentication requests.

You can also configure an authentication timeout (default is 10 minutes) to control the number of minutes before an authentication check times out. Timeouts affect the following user types differently:

- **Auth user**: The timeout countdown begins after the first authenticated session completes. If users initiate a new session before the countdown reaches the timeout threshold, they do not need to reauthenticate and the timeout countdown resets. The default timeout value is 10 minutes, and the maximum is 255 minutes. You can also set the timeout value at 0 so that the authentication period never times out.

- **Admin user**: If the length of idle time reaches the timeout threshold, the security device terminates the admin session. To continue managing the device, the admin must reconnect to the device and reauthenticate. The default timeout value is 10 minutes, and the maximum is 1000 minutes. You can also set the timeout value at 0 so that an admin session never times out.

---

**NOTE**: User authentication timeout is not the same as session idle timeout. If no activity occurs in a session for a predefined length of time, the security device automatically removes the session from its session table.

Configuring Authentication Server Redundancy

In the Redundancy tab, you can configure backup server to handle authentication requests if the primary server fails. For RADIUS servers only, you can also configure a secondary backup server (this option is not supported for SecureID servers).

For RADIUS and LDAP servers only, you can configure a Failover Revert Interval that determines how long the device uses a backup server before attempting to use the primary server again. To configure the interval, enter the number of seconds (1 to 86400); to disable the failover revert, set the interval to 0 (the device continues to use the backup server indefinitely). The interval countdown begins when the device fails over from the primary auth server to the backup or secondary backup server (RADIUS only).

Configuring Authentication for User Types

In the Identity tab, configure the user types that the authentication server supports:

- **Admin Users**
- **Firewall Auth Users**
- **XAuth Users**
- **802.1x Users**
- **L2TP Users**
For RADIUS servers, you can also configure the optional domain name checking and domain name stripping settings, as detailed in the following sections.

**Domain Name Checking**
Use domain name checking to authenticate users from a specific domain. This setting is optional and is not required to configure a RADIUS authentication server.

To configure, for Domain to Check In Username, enter the domain name (up to 45 characters). For each user authenticating to the server, the server compares the domain name in the username to specified domain (the domain is read as a string from right to left to the first @ character).

To authenticate usernames from all domains, leave this option unconfigured (blank).

**Domain Name Stripping**
Use domain name stripping to remove the domain name from usernames before sending to the authentication server. This setting is optional and is not required to configure a RADIUS authentication server. However, you might need to configure this setting when implementing a new RADIUS server with an existing network and established usernames.

To configure:

- For Separator Character, enter the separator character used in the usernames.
- For Separator Character Occurrence, enter the number of times (0 to 10) the separator character occurs in the username.

When a user attempts to authenticate, the device examines the username from right to left, then strips domain name information for the specified number of separator characters before sending the username onto the authentication server.

For example, when the Separator Character is @ and the Separator Character Occurrence is 2, the device handles the username `user1@mygrp.abc@myco.com` by stripping the characters `@mygrp.abc@myco.com` and sending only the characters `user1` to the authentication server.

If the device does not locate the separator character in the username, it does not strip the domain name from the username (usernames are passed to the authentication server as-is). Conversely, if the number of specified separator characters exceeds the number of separators found in a username, the device strips domain name information to the number of separators found (when reading right to left).

**Configuring Authentication Server Types**
In the Server Type tab, select the authentication server type (RADIUS, SecureID, LDAP) to configure specific settings for that server type:

- For RADIUS, see “Configuring a RADIUS Authentication Server” on page 501.
- For SecureID, see “Configuring a SecurID Authentication Server” on page 505.
Configuring a RADIUS Authentication Server

The Remote Authentication Dial-In User Service (RADIUS) is a protocol for an authentication server that can support up to tens of thousands of users. The security device acts as a RADIUS client that authenticates users. When users log in, the RADIUS client (the security device) prompts them for their user name and password, then compares these values with the values stored in the RADIUS database. If the values match, the RADIUS client authenticates the user and permits access to the appropriate network services.

For a RADIUS authentication server object, configure the following:

- **RADIUS Port**—The port number on the RADIUS server to which a security device sends authentication requests. The default port number is 1645.

- **RADIUS Secret**—The secret (password) shared between a security device and the RADIUS server. The RADIUS server uses the shared secret to generate a key to encrypt traffic between the security device and the RADIUS server. The security device uses the shared secret to encrypt the user’s password that it sends to the RADIUS server.

- **RADIUS Retry Timeout**—The interval (in seconds) that a security device waits before sending another authentication request to the RADIUS server if the previous request does not elicit a response. The default is three seconds.

- **RADIUS Retries**—The number of unanswered requests (access and accounting) that a security device sends before it considers the RADIUS server unreachable and fails over to a backup server. To configure, enter the number of retries (1 to 20); the default is three.

- **RADIUS Compatible with RFC 2138**—When selected, enables the authentication server to comply with RFC 2138, an older RADIUS standard, with the following considerations:
  - For operations where RFC 2865/66 and RFC 2138 are mutually exclusive, the server complies with RFC 2138 only.
  - For operations where RFC 2865/66 and RFC 2138 are both supported, the server complies with all three RFCs.
When unselected (default), the server is compatible only with the current RADIUS standards RFC 2865 and 2866.

- Enable Sending Calling-Station-ID—When selected, the security device transmits the calling station ID within the access or accounting request to the RADIUS authentication server. Because the ID identifies the originator of the call (either the IKE IP address for XAuth or the phone number of the user originating the call), you might not want to send this information to the server. By default, this option is disabled; the device does not send the calling station ID to the server.

- Length of Account Session ID Attribute—The byte length of the account-session-id, which uniquely identifies the accounting session. By default, the byte length is 11, and follows the format NS-xxxxxxxx. Because some RADIUS servers do not properly accept an 11-byte account session ID, you might want to configure a lower byte length that does not include the “NS-” prefix. To configure, enter a byte length from 6 to 10.

**Supported User Types**

A RADIUS server supports the following user types:

- Auth users
- L2TP users (authentication and remote settings)
- XAuth users (authentication and remote settings)
- Admin users (authentication and privilege assignments)
- User groups

A RADIUS server **does not** support IKE users.

**RADIUS Access-Challenge**

When a user attempts to log in using telnet, a security device can process access-challenge packets from an external RADIUS server. Access-challenge is an additional authentication level. After a username and password has been authenticated, the RADIUS server sends an access-challenge to the security device, which forwards the challenge to the user. When the user replies, the device sends a new access-request with the user’s response to the RADIUS server; if the user’s response is correct, the authentication process concludes successfully.

---

**NOTE:** Juniper Networks does not support access-challenge with L2TP.

---

**Juniper Networks Dictionary File**

A dictionary file defines vendor-specific attributes (VSAs) that you load onto a RADIUS server. After you define the VSA values, the security device can query those values when a user logs on to the device.
You must load a Juniper Networks dictionary file to enable the RADIUS server to support NetScreen-specific attributes as admin privileges, user groups, and remote L2TP and XAuth IP address, and DNS and WINS server address assignments. You do not need to load Juniper Networks dictionary file to enable RADIUS to make IP address assignments (Juniper Networks uses the standard RADIUS attribute for IP address assignments).

Juniper Networks provides two dictionary files: one for Cisco RADIUS servers and one for Funk Software RADIUS servers:

- For Funk Software RADIUS server dictionary file, go to http://www.juniper.net/customers/csc/research/netscreen_kb/downloads/dictionary/funk_radius.zip
- For Cisco RADIUS server dictionary file, go to http://www.juniper.net/customers/csc/research/netscreen_kb/downloads/dictionary/cisco_radius.zip

If using a Microsoft RADIUS server, there is no dictionary file. You must configure it as outlined in Using a Windows NT Domain / Active Directory for User Authentication Security Devices, which you can download from the Juniper customer support site.

Each Juniper Networks dictionary file contains the following specific information:

- **Vendor ID**—The Juniper Networks vendor ID (VID; also called an “IETF number”) is 3224. The VID identifies a specific vendor for a particular attribute. Some types of RADIUS server require you to enter the VID for each attribute entry, while other types only require you to enter it once and then apply it globally. Refer to your RADIUS server documentation for further information.

- **Attribute Name**—The attribute names describe individual NetScreen-specific attributes, such as NS-Admin-Privilege, NS-User-Group, and NS-Primary-DNS-Server.

- **Attribute Number**—The attribute number identifies an individual vendor-specific attribute.

- **Attribute Type**—The attribute type identifies the form in which attribute data (or “value”) appears—a string, an IP address, or an integer.

The RADIUS server automatically receives the above information when you load the Juniper Networks dictionary file onto it. To make new data entries, you must manually enter a value in the form indicated by the attribute type.

**EXAMPLE: CONFIGURING A RADIUS AUTH SERVER**

In the following example, you define an auth server object for a RADIUS server. You specify its user account types as auth, L2TP, and XAuth. You name the RADIUS server “radius1” and accept the ID number that the security device automatically assigns it. You enter its IP address, which is 10.20.1.100; and change its port number from the default port number (1645) to 4500. You define its shared secret as “A56htYY97kl”. You change the authentication timeout value from the default (10 minutes) to 30 minutes and the RADIUS retry timeout from 3 seconds to 4 seconds. You also assign its two backup servers the IP addresses 10.20.1.110 and 10.20.1.120.
In addition, you load the Juniper Networks dictionary file on the RADIUS server so that it can support queries for the following vendor-specific attributes (VSAs): user groups, admin privileges, remote L2TP and XAuth settings.

Figure 109: Configure RADIUS Auth Server

The security device sends auth, L2TP, and XAuth authentication requests to the primary RADIUS server, “radius1”, at 10.20.1.100.

If the security device loses network connectivity with the primary RADIUS server, the device redirects authentication requests to backup1 at 10.20.1.110.

If the security device cannot reach backup1, it redirects authentication requests to backup2 at 10.20.1.120.

1. In the main navigation tree, select Object Manager > Authentication Servers and click the Add icon. Enter a name, color, and comment for the authentication server.
2. Configure the RADIUS servers:
   - For Main Server, enter the IP 10.20.1.100
   - For Primary Backup Server, enter IP 10.20.1.110
   - For Secondary Backup Server, enter IP 10.20.1.120
3. For timeout, enter 30.
4. Select the following:
   - For Firewall Auth Users
   - For XAuth Users
   - For L2TP Users
5. For Server Type, select RADIUS.
6. Configure the RADIUS server properties:
   - For server port, enter 4500 (default is 1645)
   - For secret, enter A56htYY97kl
   - For retry timeout, select 4.
7. Click OK to save the RADIUS authentication server object.
8. Load the Juniper Networks dictionary file on the RADIUS server.

Configuring a SecurID Authentication Server

Security devices also support the RSA SecurID system. The device acts as a SecurID client, forwarding authentication requests to the external server for approval and relaying login information between the user and the server. Each SecurID user has three authentication credentials:

- **User Name**
- **Personal identification number (PIN)**
- **Authenticator**—a SecurID issued device with an LCD screen that displays a token code, a randomly generated string of numbers that changes every minute. The authenticator uses an algorithm known only by RSA to create the token code that appears in LCD screen; when users enter their username, their PIN, and the token code from their authenticator, the RSA ACE server also performs the same algorithm, generating a match between the server and the user.

When users log in, the SecurID client (the security device) prompts them for their user name, their PIN, and the current token code. The device compares the user input against value generated by the RSA ACE server algorithm. If the values match, the authentication is successful.

For a SecurID authentication server object, you must configure the following:

- **Authentication Port**—The port number on the SecurID ACE server to which the security device sends authentication requests. The default port number is 5500.
- **Encryption Type**—The algorithm used for encrypting communication between the security device and the SecurID ACE server (SDI or DES).
- **Client Retries**—The number of times that the SecurID client (the security device) tries to establish communication with the SecurID ACE server before aborting the attempt.
- **Client Timeout**—The length of time in seconds that the security device waits between authentication retry attempts.
- **Use Duress**—An option that prevents or allows use of a different PIN number. When this option is enabled, and a user enters a previously determined duress PIN number, the security device sends a signal to the SecurID ACE server, indicating that the user is performing the login against his or her will, possible under duress. The SecurID ACE server permits access that one time, then denies any further login attempts by that user until he or she contacts the SecurID administrator. Duress mode is available only if the SecurID ACE server supports this option.
Supported Users
A SecurID Ace server supports the following types of users and authentication features:

- Auth users
- L2TP users (user authentication; L2TP user receives default L2TP settings from the security device)
- XAuth users (user authentication; no support for remote setting assignments)
- Admin users (user authentication; admin user receives default privilege assignment of read-only)

A SecurID ACE server can store L2TP, XAuth, and device admin user accounts for authentication purposes, but cannot assign L2TP or XAuth remote settings or device admin privileges.

Configuring an LDAP Authentication Server
Lightweight Directory Access Protocol (LDAP) a protocol for organizing and accessing information in a hierarchical structure resembling a branching tree. LDAP is used to locate resources, such as organizations, individuals, and files on a network, and helps authenticate users attempting to connect to networks controlled by directory servers.

To create an LDAP authentication server object, configure the following:

- LDAP Server Port: The port number on the LDAP server to which the security device sends authentication requests. The default port number is 389.
- Common Name Identifier: The identifier used by the LDAP server to identify the individual entered in a LDAP server. For example, an entry of “uid” means “user ID” and “cn” for “common name”.
- Distinguished Name (dn): The path used by the LDAP server before using the common name identifier to search for a specific entry. (For example, c=us,o=juniper, where “c” stands for “country”, and “o” for “organization”.)

Supported Users
An LDAP server supports the following types of users and authentication features:

- Auth users
- L2TP users (user authentication; L2TP user receives default L2TP settings from the security device)
- XAuth users (user authentication; no support for remote setting assignments)
- Admin users (user authentication; admin user receives default privilege assignment of read-only)

LDAP servers cannot assign L2TP or XAuth remote settings.
Configuring User Objects

User objects represent the users of your managed devices. You can include user objects or groups in Security Policies or VPNs to permit or deny access to individuals or groups. NetScreen-Security Manager supports two types of user objects:

- **Local Users**—Users with accounts that are managed by your security devices. You can create local user groups that include multiple users to simplify user administration and make policies and VPNs easier to create.

- **External Users and External User Groups**—Users with accounts that are managed by external devices, such as RADIUS servers. You can use external users and groups to create group expressions (for details, see “Configuring Group Expressions” on page 512).

### Configuring Local Users

Local User Objects represent the user account on your security devices. To add a local user object:

1. In the navigation tree, double-click the Object Manager, select User Objects, then select Local Users. In the main display area, click the Add icon and select New > User to display the New Local User dialog box.

2. Enter a name, color, and comment for the local group.

3. Select Enable to enable authentication for this user, then configure the authentication methods for the user:
   - **XAuth.** Enables XAuth authentication for this user. If you select this option, you must also enter an XAuth password for the user.
   - **IKE.** Enables IKE authentication using one of the IKE proposals defined in the IKE Proposal Objects. If you select this option, you must also configure the IKE Share limit and authentication token.
   - **Auth.** Enables local authentication against a username and password stored in a security device’s local database. If you select this option, you must also enter an Auth password for the user.
   - **L2TP.** Enables authentication in the L2TP tunnel that the user uses to connect to the device. If you select this option, you must also enter an L2TP password for the user.

4. Click OK to save the user object.

### Configuring Local User Groups

Organize local users in groups to add multiple users at one time to a Security Policy, and to manage the members without changing the policy. To add a local user group object:

---

**NOTE:** All passwords handled by NetScreen-Security Manager are case-sensitive.
1. In the navigation tree, double-click the Object Manager, select User Objects, then select Local Users. In the main display area, click the Add icon and select New > Group to display the New Local User Group dialog box.

2. Enter a name, color, and comment for the local user group.

3. Configure the members of the group:
   - To add members, select users from the Non-members list and click Add. Use Ctrl-click to select multiple users, or click Add All to add all users in Non-members list to the group.
   - To remove members, select users in the Members list and click Remove. Use Ctrl-click to select multiple users, or click Remove All to remove all users in Members list from the group.

4. Click OK to save the local user group.

Configuring External Users

External User Objects represent users whose accounts are maintained and authenticated on devices that are not managed by NetScreen-Security Manager, such as an external RADIUS or SecureID server. When an external user is included in a Security Policy (under Authentication rule options), the security device uses the external server to authenticate that user.

To configure an external user:

1. In the navigation tree, double-click the Object Manager, select User Objects, then select External Users. In the main display area, click the Add icon and select New to display the New External User dialog box.

2. Enter a name, color, and comment for the external user.

3. Click OK to save the external user object.

Configuring External User Groups

External User Group objects represent user groups that are managed on non-security devices, such as an external RADIUS or SecureID server. When an external user group is included in a Security Policy (under Authentication rule options), the security device uses the external server to authenticate those users.

To use an external user group in a VPN, however, you must also create local user objects with IKE authentication for each external user. In phase 1 of IKE negotiations, the security device authenticates the external user group using the RADIUS server. In phase 2 of IKE negotiations, the device uses the local user object or local user group for authentication. Typically, you configure the local user object with IKE authentication and a U-FQDN (email address); during phase 2, the device prompts the user for their U-FQDN for authentication.

To add an external user group object:
1. In the navigation tree, select Object Manager > User Objects > External User Groups. In the main display area, click the Add icon and select New to display the New External Group dialog box.

2. Enter a name for the external user group. The name must match the name of the user group as configured on the external server.

3. Enter a color and comment for the external user group.

4. Configure the authentication methods for the user group:
   - XAuth. Enables XAuth authentication for the user group.
   - Auth. Enables local authentication against a username and password stored in a security device's local database.
   - L2TP. Enables authentication in the L2TP tunnel that users in the group use to connect to the device.

5. Click OK to save the new group.

EXAMPLE: USING RADIUS WITH USER GROUPS
In this example, you configure an external RADIUS auth server named radius1 and define an external auth user group named auth_grp2. You define the external auth user group auth_grp2 in two places: External RADIUS auth server “radius1”, and in NetScreen-Security Manager. For the RADIUS server, you enter the IP address 10.20.1.100 and change its port number from the default port number (1645) to 4500.

Next, you populate the auth user group “auth_grp2” with auth users on the RADIUS server only, leaving the group unpopulated in NetScreen-Security Manager. The members in this group are accountants who require exclusive access to a server at IP address 10.1.1.80. You create an address book entry for the server and name the address “midas.” Finally, you configure a Security Policy that permits only authenticated traffic from auth_grp2 to midas, both of which are in the Trust zone.

1. On the RADIUS server, load the Juniper Networks dictionary file and define auth user accounts. Use the Juniper Networks user group VSA to create the user group auth_grp2 and apply it to the auth user accounts that you want to add to that group.

NOTE: All passwords handled by NetScreen-Security Manager are case-sensitive.

2. In NetScreen-Security Manager, in the main navigation tree, select Object Manager > Authentication Servers and click the Add icon. Configure the server:
   a. For name, enter radius1. Select a color and add a comment, if desired.
b. For Main Server, enter the IP 10.20.1.100; for Primary Backup Server, enter IP 10.20.1.110; for Secondary Backup Server, enter IP 10.20.1.120.

c. For timeout, enter 30.

d. Select For Firewall Auth Users.

e. For Server Type, select RADIUS, then configure the RADIUS server:
   - For server port, enter 4500 (default is 1645)
   - For secret, enter A56hYY97kl
   - For retry timeout, select 4.

f. Click OK to save the RADIUS authentication server object.

3. Configure the External User Group in NetScreen-Security Manager:

   a. In the Object Manager, select User Objects > External User Groups.

   b. Click the Add icon to display the New External User Group dialog box. Configure the following, then click OK:

      - For Name, enter auth_grp2.
      - For Color, select red.
      - For Comment, enter Accountant Access.
      - Enable Auth.

4. Add the Address Object that represents the Accounting Server:

   a. In the Object Manager, select Address Objects. Click the Add icon and select Host. The New Host dialog box appears.

   b. Configure the following, then click OK:

      - For Name, enter Midas.
      - For Color, select orange.
      - For Comment, enter Accounting Server.
      - Select IP, then enter the IP Address 10.1.1.80.

5. Configure a firewall rule to use the RADIUS authentication server object to authenticate traffic between the external user group and the Midas server, as shown below:
An IP pool object contains IP ranges (a range of IP addresses within the same subnet). You use IP Pool objects to assign IP addresses to L2TP users in L2TP VPNs or local users on a specific device. The IP pool you select for the VPN or the local user determines the range of IP addresses the device can assign to the L2TP RAS user when the user connects to the L2TP VPN.

**NOTE:** For details on configuring XAuth and L2TP local users on a device, see “Configuring L2TP Local Users” on page 349.

An IP range includes the following:

- **Start IP**—The beginning of the range of IP addresses included in the pool, inclusive. The Start IP must always be lower than the End IP.

- **End IP**—The end of the range of IP addresses included in the pool, inclusive. The End IP must always be higher than the Start IP.

**Using Multiple IP Ranges**

An IP Pool object can contain multiple, non-sequential IP ranges. You might need to use multiple ranges to accommodate large numbers of RAS users in a VPN.
You can configure up to 256 IP ranges within a single IP Pool object. You can add any number of IP Pool objects.

**NOTE:** Devices running ScreenOS 5.1 or earlier versions do not support multiple IP pool ranges. When you include a multi-range IP pool object in a device configuration or VPN for a device running ScreenOS 5.1 or earlier version, the device automatically uses the first IP range defined in the IP Pool object.

To modify or delete an IP range from an IP Pool object, you must first ensure that no IP within the range is currently in use by any managed device. If you change or delete an IP range that contains a used IP address, the device using the IP generates an error during device update (error message appears with the Job Manager dialog box for the update).

**EXAMPLE: CONFIGURING AN IP POOL OBJECT**

In this example, you configure an IP pool with the ranges 1.1.1.1-1.1.1.10 and 2.2.2.2-2.2.2.20.

1. In the navigation tree, select Object Manager > IP Pools.

2. In the main display area, click the Add icon. The New IP Pool dialog box appears. Configure as detailed below:

   - For Name, enter L2TP User Group 1.
   - For Color, select orange.
   - For Comment, enter IPs for usergrp 1.

3. In the IP Pool dialog box, click the Add icon to configure the first IP pool range. The New IP Pool Name dialog box appears. Configure as detailed below, then click OK:

   - For Start IP, enter 1.1.1.1.
   - For End IP, enter 1.1.1.10.

4. In the IP Pool dialog box, click the Add icon to configure the second IP pool range. The New IP Pool Name dialog box appears. Configure as detailed below, then click OK:

   - For Start IP, enter 2.2.2.2.
   - For End IP, enter 2.2.2.20.

5. Click OK again to save the IP Pool object and return to Object Manager.

**Configuring Group Expressions**

Group expressions are statements that set conditions for authentication requirements, enabling you to combine multiple external user objects. You can create group expressions using the operator OR, AND, or NOT to combine user objects, user group objects, or other group expressions to define:
Alternatives for authentication ("a" OR "b")

Requirements for authentication "a" AND "b"

Exclusions of a user, user group, or another group expression (NOT "c").

**NOTE:** The user and user groups you reference in the group expressions must be external users that are stored on an external RADIUS server. (A RADIUS server enables a user to belong to more than one user group).

The operators have different meanings depending on the type of user object you are using in the Security Policy, as detailed below:

Table 29: Group Expression Operators

<table>
<thead>
<tr>
<th>User Objects</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OR</td>
<td>If the Security Policy defines authentication for &quot;a&quot; or &quot;b&quot; user objects, the security device authenticates the user if it is either &quot;a&quot; or &quot;b&quot;.</td>
</tr>
<tr>
<td>AND</td>
<td>Requires one of the two objects in the expression to be either a user group or a group expression (a single user cannot be both user &quot;a&quot; and user &quot;b&quot;). If the Security Policy defines authentication for &quot;a&quot; AND a member of group &quot;b&quot;, the security device authenticates the user only if those two conditions are met.</td>
</tr>
<tr>
<td>NOT</td>
<td>If the Security Policy defines authentication for any user object that is not the &quot;c&quot; user (NOT &quot;c&quot;), the security device authenticates all users except the &quot;c&quot; user.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>User groups</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OR</td>
<td>If the Security Policy defines authentication for user group &quot;a&quot; or user group &quot;b&quot;, the security device authenticates the user if it belongs to either &quot;a&quot; or &quot;b&quot; user group.</td>
</tr>
<tr>
<td>AND</td>
<td>If the Security Policy defines authentication for user group &quot;a&quot; AND user group &quot;b&quot;, the security device authenticates the user only if it belongs to both user groups.</td>
</tr>
<tr>
<td>NOT</td>
<td>If the Security Policy defines authentication for any user group that is not group &quot;c&quot; (NOT &quot;c&quot;), the security device authenticates all users except those that belong to the &quot;c&quot; user group.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Group expressions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OR</td>
<td>If the Security Policy defines authentication for user objects that match the description of group expression &quot;a&quot; OR group expression &quot;b&quot;, the security device authenticates the user if either group expression references that user.</td>
</tr>
<tr>
<td>AND</td>
<td>If the Security Policy defines authentication for user objects that match the description of group expression &quot;a&quot; AND group expression &quot;b&quot;, the security device authenticates the user only if both group expressions reference that user.</td>
</tr>
<tr>
<td>NOT</td>
<td>If the Security Policy defines authentication for user objects that do not match the description of group expression &quot;c&quot; (NOT &quot;c&quot;), the security device authenticates all users except those that match the group expression.</td>
</tr>
</tbody>
</table>

**Configuring Group Expressions**

Because a group expression references external user objects and/or external user groups, you must first create those user object and groups before you can use them in a group expression. You cannot reference local user object or local user object groups in a group expression.

To add a group expression:
1. In the navigation tree, double-click Object Manager and select Group Expressions.

2. In the main display area, click the Add icon and select New. The New Group Expression dialog box appears.

3. Enter a name, color, and comment for the group expression.

4. Select the operator you want to use in the expression (OR, AND, NOT) and then configure the Operands:

   - For NOT expressions, use Operand 1 to select the user object, group, or expression that cannot be present for a successful match. Because the operation is exclusion, you do not need to configure Operand 2.

   - For AND expressions, use Operand 1 and Operand 2 to select the two user object, group, or expression that must be present for a successful match.

   - For OR expressions, use Operand 1 and Operand 2 to select the two user object, group, or expression, one of which must be present for a successful match.

5. Click OK. The group expression object appears in the Object Manager.

After you have created a group expression object, you can use that object in the Authentication rule options. For details, see “Configuring Firewall Rule Options” on page 542.

EXAMPLE: CREATING A GROUP EXPRESSION

In this example, you configure a group expression to authenticate all users that belong to your Sales group and your Marketing group, then add the expression to a Security Policy that provides access to your protected networks.

1. First, create two external user group objects: one to represent the Sales users and the other to represent the Marketing users, as shown below:

   ![Figure 111: Configure External User Groups for Sales and Marketing](image)

<table>
<thead>
<tr>
<th>Name</th>
<th>Auth</th>
<th>L2TP</th>
<th>XAuth</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Marketing Group</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>All Marketing</td>
</tr>
<tr>
<td>Sales Group</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>All sales</td>
</tr>
</tbody>
</table>

2. Next, create a group expression object that reference both the Sales and Marketing group, as shown below:
Configuring Remote Settings

A remote settings object defines the DNS and WINS servers that are assigned to L2TP RAS users after they have connected to the L2TP tunnel. You can use remote settings objects in an L2TP VPN, and when configuring a local user on a specific device.

NOTE: For details on configuring XAuth and L2TP local users on a device, see “Configuring L2TP and XAuth Local Users” on page 349.
Security devices incorporate DNS (domain name server) and WINS support to permit the use of domain names as well as IP addresses for identifying locations. A DNS or WINS server keeps a table of the IP addresses associated with domain names. Using DNS or WINS, you can reference locations by their domain name (www.juniper.net) in addition to using a routeable IP address (such as 209.125.148.136).

Before you can use DNS or WINS for domain name/address resolution in a VPN, you must create remote settings for the DNS or WINS servers (primary and secondary).

To configure a remote setting, select Remote Settings and click the Add icon. Enter a name, color, and comment for the object, then configure the following parameters:

- **DNS1**—Enter the IP address of the primary DNS server.
- **DNS2**—Enter the IP address of the secondary DNS server.
- **WINS1**—Enter the IP address of the primary WINS server.
- **WINS2**—Enter the IP address of the secondary WINS server.

### Configuring NAT Objects

A global NAT object contains references to device-specific NAT configurations, enabling multiple devices to share a single object.

Use the Device Manager to configure NAT for each device, then create a global NAT object that includes the device-specific NAT configuration. The single global NAT object represents multiple device-specific NAT objects; for example, a global DIP represents multiple device-specific DIPs. However, a global NAT object can contain only one device-specific NAT object from the same device.

Use global NAT objects in VPNs; when you install the VPN on a device, that device automatically replaces the global NAT object with its device-specific NAT configuration. Before you configure a shared NAT object, ensure that you have configured the MIP, VIP, or DIP on the device itself.

### Configuring DIP Objects

In Object Manager, select NAT Objects > DIP and click the Add icon. Enter a name, color, and comment for the object, then click the Add icon to specify the device-specific DIP:

- **Device**—Select the security device that includes the DIP.
- **Interface or DIP Group**—Select the interface or DIP group for the device.
  - For interface, select the interface on the device and the dynamic IP address configuration for that interface.
  - For DIP group, select the dynamic IP group configuration for that device.
If no values appear in the pull-down menu for interface, DIP, or DIP group, ensure that you have configured DIP correctly in the Device Manager.

You can add multiple device DIPs to a single global DIP object (one DIP per each device).

For details on configuring a DIP object and an example, see “Configuring DIPs” on page 237. For details on configuring a DIP group and an example, see “Configuring DIP Groups” on page 273.

Configuring MIP Objects
In Object Manager, select NAT Objects > MIP and click the Add icon. Enter a name, color, and comment for the object, then click the Add icon to specify the device-specific MIP:

- Device—Select the security device that includes the MIP.
- Interface—Select the interface on the device that uses the mapped IP address.
- MIP—Select the mapped IP address configuration for that interface.

If no values appear in the pull-down menu for interface or MIP, ensure that you have configured MIP correctly in the Device Manager. You can add multiple device MIPs to a single global MIP object.

For details on configuring a MIP object and an example, see “Configuring MIPs” on page 230.

Configuring VIP Objects
In Object Manager, select NAT Objects > VIP and click the Add icon. Enter a name, color, and comment for the object, then click the Add icon to specify the device-specific VIP configuration:

- Device—Select the security device that includes the VIP.
- Interface—Select the interface on the device that uses the virtual IP address.
- VIP—Select the virtual IP address configuration for that interface.

If no values appear in the pull-down menu for interface or VIP, ensure that you have configured VIP correctly in the Device Manager. You can add multiple device VIPs to a single global VIP object.

For details on configuring a VIP object and an example, see “Configuring VIPs” on page 233.

Configuring Certificate Authorities
A digital certificate is an electronic means for verifying your identity through the word of a trusted third party, known as a Certificate Authority (CA). NetScreen-Security Manager simplifies creating and managing certificates:
- Use the same CA server for multiple devices. Create a single CA object for each CA server you use, then use that object for those devices.

- Generate a local and CA certificate in one click using SCEP.

- Use OCSP to automatically check for revoked certificates (ScreenOS 5.x devices only)

- Use a certificate chain that includes a root CA and subordinate CA (CA group)

A CA object represents the CA server you want to use to authenticate the identity of your VPN member. You can use an independent or internal CA server:

- Independent CA server—Owned and operated by an independent CA. The independent CA provides the IP addresses of their CA and CRL servers. You submit a local certificate request to the independent CA and provide your local certificate information.

- Internal CA server—Owned and operated by your company. You provide the IP addresses of the CA and CRL servers and local certificate information.

You can obtain a CA certificate file (.cer) from the CA that issued the local certification, then use this file to create a Certificate Authority object. Then, install this CA certificate on the managed device using NetScreen-Security Manager. Because the CA certificate is an object, however, you can use the same CA for multiple devices, as long as those devices use local certificates that were issued by that CA.

Alternatively, you can use SCEP to configure the device to automatically obtain a CA certificate at the same time it receives the local certificate. For details, see “Configuring Certificates” on page 366.

Using Certificate Authorities

You must use obtain and install a CA certificate on each VPN member to authenticate the local device certificates on your managed devices.

Configuring Certificate Authorities

After you have obtained a CA Certificate file (.cer) from your CA, use this file to create a Certificate Authority Object. In Object Manager, select Certificate Authorities, then click the Add icon to display the New CA Certificate dialog box. Enter a name for the CA Certificate, then click Load CA certificate and load the appropriate .cer file. NetScreen-Security Manager uses the information in the .cer file to automatically complete the Subject Name, Issued By, and Expired On fields.

Complete the remaining settings:

- X.509 Certificate Path Validation Level—X509 contains a specification for a certificate which binds an entity’s distinguished name to its public key through the use of a digital signature.
  - Full. Use full validation to validate the certificate path back to the root.
- Partial. Use partial validation to validate the certificate path only part of the way to the root.

- Revocation Check
  - Check for revocation. Select this option to enable revocation checking.
  - Do not check for revocation. Select this option to disable revocation checking.

- Revocation Checking Method—If you enabled revocation checking, you can select the checking method to use. If you did not enable revocation checking, these fields are unavailable.
  - CRL. Use a Certificate Revocation List when you want to keep a local copy of the revoked certificates on the managed device. This method enables the device to check for revoked certificates quickly; to accept the certificate if no revocation information is found, also enable Best Effort.
  - OCSP. Use the Online Certificate Status Protocol when you want the managed device to access a remote OCSP server to check for revoked certificates. Because the OCSP server dynamically updates its list of revoked certificates, this method provides the most up-to-date information; to accept the certificate if no revocation information is found, also enable Best Effort.
  - Best Effort. Enable this option to check for revocation accept the certificate if no revocation information is found.

- CRL Settings—Configure the default setting for the Certificate Revocation List.
  - Refresh Frequency. Select the frequency that the device contacts the CA to obtain a new CRL list: Daily, Weekly, or Monthly.
  - LDAP server. Provide the IP address of the external LDAP server that manages the CRL.
  - URL address. Provide the URL address of your internal LDAP server that provides the CRL.

- OCSP—Configure the Online Certificate Status Protocol to dynamically check for revoked certificates.
  - Certificate Verification.
  - No revoke status check for CA delegated signing cert.
  - URL of OCSP Responder. Provide the URL address of the OCSP server.

- SCEP—Configure Simple Certificate Enrollment Protocol to get a local certificate automatically.
  - CA CGI. Enter the URL address of the Certificate Authority Certificate Generation Information.
RA CGI. Enter the URL address of the Registration Authority Certificate Generation Information that the security device contacts to request a CA certificate.

CA IDENT. Enter the name of the certificate authority to confirm certificate ownership.

Challenge. Enter the challenge word(s) sent to you by the CA that confirm the security device identity to the CA.

CA Certificate Authentication. (Auto or Manual)

Polling Interval. (Poll or Do not poll).

Certificate Renewal. Define the number of times a certificate can be renewed.

Click OK to complete the CA Object.

Configuring CRL Objects

A Certificate Revocation List (CRL) identifies invalid certificates. You can obtain a CRL file (.crl) from the CA that issued the local certification and CA certificate for the device, then use this file to create a Certificate Revocation List object.

You must install the CRL on the managed device using NetScreen-Security Manager. Because the CRL is an object, however, you can use the same CRL for multiple devices, as long as those devices use local and CA certificates that were issued by that CA.

Using CRLs

You can use a CRL object in a VPN to check for VPN members using revoked certificates.

Configuring CRLs

After you have obtained a CRL file (.crl) from your CA, use this file to create a Certificate Revocation Object.

In Object Manager, select CRLs, then click the Add icon to display the New CRL dialog box. Enter a name for the CRL, then click Load CRL and load the appropriate .crl file. NetScreen-Security Manager uses the information in the .crl file to automatically complete the Issued By and Expire On fields. Click OK to complete the CRL object.

Configuring Protected Resources

A protected resource combines network components, network services, a traffic direction, and the security devices that protect those components and services. Protected resources are the source and destination addresses of a policy-based VPN.
Protected resources consist of three elements:

- **IP Address**—The address represents the computer, network, or range of addresses to be considered part of this protected resource. The Address can be an individual host, a network, or an address group.

- **Network Service**—Services are the protocols (HTTP, FTP) that communicate over a network. The service can be an individual service or a service group.

- **Traffic Direction**—Traffic direction is determined by the IP address that initiates the connection:
  - Client connections are outgoing (outbound) from the protected network.
  - Server connections are incoming (inbound) to the protected network.
  - To protect incoming and outgoing traffic, select Both.

- **Security device**—The device that protects the network component and server. If the resource can be reached through more than one device, add multiple devices to the resource. When you add a protected resource to a VPN, the devices in the protected resource are included in the VPN.

Each protected resource represents an address or a range of addresses on your network. Each resource also can specify a service (such as FTP or NSF). Therefore, the protected resource is the destination for all traffic using the selected service to the selected address.
You can have more than one protected resource for a single address or range of addresses. That way you can individually manage different services traffic to the same destination separately.

**Creating Protected Resources**

To add a protected resource object:

1. In the navigation tree, select VPN Manager > Protected Resources. In the main display area, click the Add icon to display the Protected Resource dialog box.

2. Enter a name for the protected resource.

3. Select the services you want to permit to this resource, such as FTP, HTTP, NFS, and so on. Select Any to permit all services.

4. Select the initiator of the permitted service: Server, a Client, or Both.

5. Select the address object or address group for the resource.

6. Add the security device through which traffic can reach the protected resource:
   a. In the Security Gateway area, click the Add icon to display the Security Gateway dialog box.
   b. Select security device or device group
   c. Select the security zone on the security device that contains the address objects.
   d. Click OK to add the security gateway to the protected resource.

You can add multiple security gateways to provide redundant access for the protected resource.

**Editing Protected Resources**

You can edit protected resources to accommodate changes in your network:

- If you make changes to a protected resource object that is used in a VPN, NetScreen-Security Manager automatically generates new configuration and propagates your changes to all affected security devices.

- If you change the security device that protects a resource, NetScreen-Security Manager removes the previous security device from all affected VPNs and adds the new security device. However, NetScreen-Security Manager does not configure the VPN topology for the new security device—you must reconfigure the topology to include the new device manually.
Configuring IKE Proposals

In an AutoKey IKE VPN, you can use the Internet Key Exchange (IKE) protocol to generate and distribute encryption keys and authentication algorithms to all VPN nodes. IKE automatically generates new encryption keys for the traffic on the network, and automatically replaces those keys when they expire. Because IKE generates keys automatically, you can give each key a short life span, making it expire before it can be broken. By also exchanging authentication algorithms, IKE can confirm that the communication in the VPN tunnel is secure.

Because all security parameters are dynamically assigned, VPN nodes must negotiate the exact set of security parameters that will be used to send and receive data to other VPN nodes. To enable negotiations, each VPN node contains a list of proposals; each proposal is a set of encryption keys and authentication algorithms. When a VPN node attempts to send data through the VPN tunnel, IKE compares the proposals from each VPN node and selects a proposal that is common to both nodes. If IKE cannot find a proposal that exists on both nodes, the connection is not established.

IKE negotiations include two phases:

- In Phase 1, two members establish a secure and authenticated communication channel.
- In Phase 2, two members negotiate Security Associations for services (such as IPsec) that require key material and/or parameters.

By default, NetScreen-Security Manager includes several common IKE phase1 and phase 2 proposals. To view these proposals, open VPN Manager and select IKE Phase1 Proposals or IKE Phase2 Proposals.

Creating Custom IKE Phase1 Proposals

Create a custom proposals for a specific combination of authentication and encryption that is not available in the predefined proposals, or to match the name of proposals on a non-security device.

To create a custom IKE Phase1 proposal, select Custom IKE Phase1 and click the Add icon. Enter a name and choose a color for the object, then configure the following settings:

- **Authentication Method**—Select the authentication method.
  - Preshared Key. Use this option to generate an ephemeral secret and authenticate data using MD5 or SHA hash algorithms against the secret.
  - RSA Certificate.
  - DSA Certificate.
  - Diffie-Hellman Group—The Diffie-Hellman group provides asymmetric encryption to encrypt the keys needed to decrypt the data. The larger the modulus of the group, the more secure the generated key is—and the more time it takes to generate the key. Select the group that meets your security requirements and user needs.
Group 1. Uses a 768-bit modulus.
Group 2. Uses a 1024-bit modulus.
Group 5. Uses a 1536-bit modulus.

Encryption Algorithm—Select the algorithm that meets your security requirements:

- DES-CBC
- 3DES-CBC
- AES-CBC (128 Bits)
- AES-CBC (192 Bits)
- AES-CBC (256 Bits)

Hash Algorithm—Select the algorithm that meets your security requirements.

- MD5. Authenticate data using Message Digest version 5.
- SHA-1. Authenticate data with Secure Hash Algorithm-1.

Lifetime—Enter the number of seconds before the key is regenerated. The default value is 28800 seconds (8 hours).

Click OK to add the custom IKE object to the management system.

Creating Custom IKE Phase2 Proposals

Create a custom proposals for a specific combination of authentication and encryption that is not available in the predefined proposals, or to match the name of proposals on a non-security device.

To create a custom IKE Phase2 proposal, select Custom IKE Phase2 and click the Add icon. Enter a name and choose a color for the object, then configure the following settings:

- Perfect Forward Secrecy—PFS ensures that a single key permits access to data protected by that single key. The key used to protect transmission of data and the material used to create that key are used only once and are not used to derive additional keys. Select the DH group to encrypt the key:

  - No Perfect Forward Secrecy.
  - Diffie-Hellman Group 1.
  - Diffie-Hellman Group 2.
- Diffie-Hellman Group 3.

- Lifetime (Seconds)—Enter the number of seconds before the key is regenerated. The default value is 3600 seconds (8 hours).

- Lifesize (KB)—Enter the number of bytes permitted through the connection before the key is regenerated. A value of 0 (the default) means no limit.

- Encryption (ESP) or Authentication (AH) Algorithm.

  - Select ESP to configure encryption and authentication, then select the desired algorithms.

  - Select AH to configure authentication only, then select the desired algorithm.

**NOTE:** We strongly recommend that you do not use null AH with ESP.

Click OK to add the custom IKE object to the management system.
Firewall rules define access to your network, including permitted services, users, and time periods. You can also use firewall rules to control the shape of your network traffic as it passes through the firewall, or to log specific network events. Multicast rules permit multicast control traffic, such as IGMP or PIM-SM messages, to cross Juniper Networks security devices. Multicast rules permit multicast control traffic only; to permit data traffic (both unicast and multicast) to pass between zones, you must configure firewall rules. Finally, IDP rules (supported on ISG 2000 and 1000 security devices running ScreenOS 5.0.0-IDP1) detect and prevent attacks against protected devices or applications on your network.

The following sections are in this chapter:

- About Security Policies
- Creating a Security Policy
- Configuring Firewall Rules
- Configuring Multicast Rules
- Configuring Antivirus Rules
- Configuring Antispam Rules
- Configuring IDP Rules
- Configuring Exempt Rules
- Configuring Backdoor Rules
- Installing Security Policies
- Managing Rules and Policies

Because all incoming and outgoing network traffic passes through your firewall, it is the ideal location to control the traffic flowing on your network. Creating Security Policies enables you to define what type of traffic should be permitted on your network, as well as how that traffic is treated while inside. A Security Policy can contain firewall rules (in the Zone and Global rulebases), multicast rules (in the Multicast rulebase), and IDP rules (in the IDP, Exempt, and Backdoor Detection rulebases).
Using Juniper Networks NetScreen-Security Manager features like device groups, zone exceptions, and application-level detection, you can create a single, efficient Security Policy that manages multiple security devices.

## About Security Policies


Using the NetScreen-Security Manager UI, you can configure rules in up to six rulebases (Zone, Global, Multicast, IDP, Exempt, and Backdoor Detection) for each Security Policy. Each rule in a rulebase is a row; you configure the columns in the row to define the rule parameters, such as traffic match conditions, action, and logging requirements. By default, each rulebase displays a subset of available columns for each rule. This mode, known as Compact Mode, contains columns in which you can configure typical rule parameters. To see additional columns, change the mode of the Security Policy to Expanded: From the menu bar, select View > Expanded Mode. You can set a different mode for each Security Policy.

After you create a Security Policy by building rules in one or more rulebases, you can assign that policy to specific security devices. For details on assigning a policy to a device, see "Assigning a Security Policy to a Device" on page 577.

NOTE: In the ScreenOS WebUI and CLI, a Security Policy is a single statement that defines a source, destination, zone, direction, and service. In NetScreen-Security Manager, those same statements are known as rules, and a Security Policy is a collection of rules.

## About Rulebases

A rulebase is a set of rules that define how the security device handles traffic. NetScreen-Security Manager supports three firewall rulebases and three IDP rulebases, as detailed in the following sections. A Security Policy can contain only one instance of any rulebase type.

By default, the predefined roles System Administrator and Domain Administrator can view and edit all rulebases and the Read-Only System Administrator and Read-Only Domain Administrator can only view rulebases. When creating a custom role, you can include permissions to view or edit individual rulebases.

NetScreen-Security Manager supports the following firewall rulebases:

- **The Zone rulebase**—Contains rules that apply to traffic from one specific zone to another. Create a firewall rule in the zone-specific rulebase when you need to control traffic between specific zones. The zone-specific rulebase can contain firewall rules, VPN rules, and VPN links.

- **The Global rulebase**—Contains rules that are valid across all zones. Create a firewall rule in the global rulebase when you need to control specific traffic across the entire firewall. The global rulebase can contain only firewall rules.
The Multicast rulebase—Contains rules that enable IGMP proxy or PIM-SM multicast control traffic between zones.

For Zone firewall rules that permit network traffic, you can enable IDP in the rule to pass the permitted traffic to the IDP rulebases. Use IDP rules to direct an IDP-capable security device to further inspect the traffic for known attacks and protocol anomalies.

NetScreen-Security Manager supports the following IDP rulebases:

- **IDP**—This rulebase protects your network from attacks by using attack objects to detect known and unknown attacks. Juniper Networks provides predefined attack objects that you can use in IDP rules. You can also configure your own custom attack objects. For more information about IDP attack objects, see “Working with IDP Attack Objects” on page 453.

  **NOTE:** Juniper Networks updates predefined attack objects on a regular basis to keep current with newly-discovered attacks. For more information about updating attack objects, “Updating the Attack Object Database” on page 416.

- **Exempt**—This rulebase works in conjunction with the IDP rulebase to prevent unnecessary alarms from being generated. You configure rules in this rulebase to exclude known false positives or to exclude a specific source, destination, or source/destination pair from matching an IDP rule. If traffic matches a rule in the IDP rulebase, IDP attempts to match the traffic against the Exempt rulebase before performing the action specified.

- **Backdoor Detection**—This rulebase protects your network from mechanisms installed on a host computer that facilitates unauthorized access to the system. Attackers who have already compromised a system typically install backdoors (such as Trojans) to make future attacks easier. When attackers send and retrieve information to and from the backdoor program (as when typing commands), they generate interactive traffic that IDP can detect.

  **NOTE:** If you import the ISG 2000 or ISG 1000 device into NetScreen-Security Manager, the imported device configuration does not include the IDP, Exempt, or Backdoor rulebases.

**Rule Execution Sequence**

The rules in all rulebases combine to create a Security Policy. Security devices process and execute firewall and VPN rules in the following order:

1. Zone rulebase
2. Global rulebase
3. Multicast rulebase

Security Devices process and execute IDP rules in the following order:

1. Exempt rulebase
2. IDP rulebase
3. Backdoor rulebase

**About Rules**

A rule is a statement that defines a specific type of network traffic; traffic must meet the rule requirements before it is permitted to pass through the security device. By default, all security devices deny all traffic.

When traffic passes through the security device, the device attempts to match that traffic against its list of rules. Network traffic that matches this list of requirements is considered to “match” the rule, and the device performs the action specified in the rule. If any requirement is not met, the network traffic does not match, and is denied.

Using the NetScreen-Security Manager UI, you can create intrazone firewall rules, global firewall rules, multicast rules, VPN rules, and VPN links for all security devices; for ISG 2000 and ISG 1000 security devices, you can also create IDP rules, exempt rules, and backdoor detection rules. Each Security Policy (all rulebases combined) can contain a maximum of 40,000 rules.

**About Firewall Rulebases**

You create rules in the firewall rulebases to enable access across your networks by permitting or denying specific network traffic flowing from one zone to another zone. After you have added your security device as a device in NetScreen-Security Manager, you can create rules in the firewall rulebases of your Security Policy.

You can build multiple firewall rules in both firewall rulebases for a single device; these rules combine to create a Security Policy that determines how your security device handles traffic. To simplify your Security Policy, use device groups to build access rules that apply to all your perimeter security devices, then apply the entire policy to the perimeter device group.

**Firewall Rules (Zone and Global)**

Within a firewall rule, you specify where the traffic is coming from, where it is going, and what service it is using. You can also use firewall rules to authenticate users, monitor network traffic flowing between zones, or set a schedule on a firewall rule that controls the time period that the rule is applied to network traffic.

**NOTE:** On Juniper Networks vsys devices, rules defined in the root system do not affect rules defined in virtual systems.

When creating firewall rules, consider the type, location, and functionality of each security device in your network. Typically, a single Security Policy for multiple devices works well for devices that perform similar functions, such as perimeter firewalls. However, you might want to create a separate Security Policy per device when the management system contains separate administrators with regional responsibilities, or when you need to troubleshoot a device issue (use one Security Policy per device to enable an admin to troubleshoot on one device without making policy changes on other devices).
A firewall rule must contain the following elements:

- **Direction**—The direction that the traffic flows between two zones; all traffic flows from a source zone to a destination zone. You can select any zone for source or destination; however, the zones must be valid for the security devices you select in the Install On column of the rule. You can also use zone exceptions to specify unique to and from zones for each device.

- **Source address**—The address that initiates the traffic.

- **Destination address**—The address that receives the traffic.

- **Service**—The application-level protocol that the traffic uses to transmit data.

- **Action**—The action the security device performs when it receives traffic that matches the direction, source, destination, and service.

- **Install On**—The security device on which the firewall rule is installed. You can install the same rule on multiple devices.

To begin configuring firewall rules for your managed devices, see “Configuring Firewall Rules” on page 536.

**VPN Links and Rules**

The rules for your rule-based VPNs appear in the Zone rulebase.

- **Use VPN Links for VPNs created in VPN Manager**—By default, VPN Manager autogenerated rules are implicitly executed as the first rule in the Zone rulebase, even though they do not appear. Because VPN Manager autogenerates the access rules for the VPN, you do not need to manually create them in the rulebase itself. However, to specify the exact location of the autogenerated rules in your rulebase, you can add a VPN link anywhere in the Zone rulebase.

- **Use VPN Rules for VPNs created manually**—If you did not use VPN Manager to create a rule-based VPN, you must manually add the VPN rules to create the VPN tunnel. You can place VPN rules anywhere in the Zone rulebase.

Because routing-based VPNs are on always-on connection between two or more termination points, you do not need VPN rules to create the routing-based VPN tunnel. However, you might want to create access rules to control the flow of traffic in a routing-based VPN tunnel. For details on adding VPN links or VPN rules, see Chapter 10 “Configuring VPNs”.

**About Rule Groups**

A rule group is a user-defined grouping of rules within the Zone rulebase. Combining rules into a rule group can help you better manage rules. For example, you might want to combine your VPN rules in a single rule group, or combine all rules that manage traffic from a specific interface on the security device.
You can add, edit, and delete rule groups; however, deleting a rule group also deletes all rules within that group. You can create multiple rule groups (40,000 rules max in a Security Policy). NetScreen-Security Manager supports one level of rule groups; you cannot create a rule group within a rule group.

**NOTE:** You can create rule groups only in the Zone rulebase; the Global, Multicast, IDP, Exempt, and Backdoor Detection rulebases do not support rule groups.

For details on using rule groups, “Using Rule Groups” on page 585.

**About the Multicast Rulebase**

By default, security devices do not permit multicast control traffic such as IGMP or PIM-SM messages. If you run IGMP proxy or PIM-SM on your network, you must configure rules in the Multicast rulebase to explicitly permit multicast control traffic between zones.

You can also configure multicast rules to translate multicast addresses. For example, to translate a multicast group address in an internal zone to a different address on the outgoing interface, specify both the original multicast address and the translated multicast group address in a multicast rule.

When you create a multicast rule, you must specify the following:

- **Source zone**—The zone from which traffic initiates.
- **Destination zone**—The zone to which traffic is sent.
- **Multicast group**—The multicast group or access list that specifies the multicast groups for which you want the security device to permit multicast traffic.

Multicast rules control the flow of multicast control traffic only. To permit data traffic (both unicast and multicast) to pass between zones, you must configure rules in a firewall rulebase.

**NOTE:** You cannot create rule groups within the Global or Multicast rulebases.

To begin configuring multicast rules for your managed devices, see “Configuring Multicast Rules” on page 553.

**About IDP Rulebases**

For IDP-capable security devices, such as the ISG 2000 or ISG 1000 running ScreenOS 5.0.0-IDP1, you can enable IDP in a zone or global firewall rule to direct permitted traffic to the IDP rulebases. If you do not enable IDP in a firewall rule for a target device, you can still configure rules in IDP rulebases, but you cannot apply the IDP rules when you update the Security Policy on the target security devices.

When configuring IDP in a firewall rule, consider the following:

- The firewall action must be permit. You cannot enable IDP for traffic that the security device denies or rejects.
Only traffic that is permitted by the firewall rule is passed to the IDP rulebases. The security device does not forward denied traffic to IDP rulebases.

You cannot configure DI for the rule; when you install the IDP license on an ISG 2000 or ISG 1000 device running ScreenOS 5.0.0-IDP1, DI is automatically disabled on the device.

**NOTE:** The Attack Profile Settings only apply to the Deep Inspection (DI) feature on security devices.

To enable IDP in a firewall rule, right-click in the Rule Options column for the zone or global firewall rule and select DI Profile/Enable IDP. The DI Profile/Enable IDP dialog box appears (by default, IDP is disabled). Select Enabled to enable IDP for traffic that matches the firewall rule, then select the mode in which you want IDP to operate:

- **In inline mode,** IDP is directly in the path of traffic on your network and can detect and block attacks. For example, you can deploy the security device with integrated FW/VPN/IDP capabilities between the Internet and an enterprise LAN, WAN, or special zones such as DMZ. This is the default mode.

- **In inline tap mode,** IDP receives a copy of a packet while the original packet is forwarded on the network. IDP examines the copy of the packet and flags any potential problems. IDP’s inspection of packets does not affect the forwarding of the packet on the network.

**Managing Security Policies**

After you have created a Security Policy, you can:

- Modify individual rules in each rulebase, such as changing rule order (determine the order that rules are applied to network traffic by placing the rules in the desired sequential order), disabling a rule, negating source or destination addresses (ScreenOS 5.x devices only), and so on.

- Validate a Security Policy before installing it on your managed devices.

- Merge multiple Security Policies into a single policy for easier management. For example, after importing (or re-importing) devices into the management system, you might want to merge their imported policies into a single policy for all devices.

- Export the policy to an HTML file.

For details on managing your Security Policies, see “Managing Rules and Policies” on page 582.

**Creating a Security Policy**

When creating a Security Policy, consider the following:
Creating a Security Policy

Objects—Before creating a Security Policy, you should first use Object Manager to create objects representing your network components, custom services, custom attack objects, and so on. You use these objects when configuring rules within the policy.

Templates—When adding a new Security Policy, to “copy” an existing policy or if you expect to configure IDP rules as part of the Security Policy, consider using a policy template.

Rulebases—After adding a Security Policy, only the Zone rulebase (default rulebase) is automatically included in the policy (unless you are using a template). To create rules in the global, multicast, or IDP rulebases, you must manually add those rulebases to the policy.

The following sections detail these options.

Configuring Objects For Rules

Objects are reusable logical entities that represent specific settings that you can reuse in multiple areas in the NetScreen-Security Manager UI. Within rules, you use objects to define the source, destination, and service, as well as to specify settings for rule options, such as WEB Filtering or attack protection.

For some object types, such as services and IDP attack objects, NetScreen-Security Manager contains a database of predefined objects. If the predefined objects do not meet your networking requirements, you can create custom objects and add them to the object database. For other object types, such as address objects, DI profiles, and Global MIPS, no predefined objects exist; before you can use one of these objects in a rule, you must create the object in Object Manager.

For details on all predefined object settings and creating custom objects, see “Configuring Objects” on page 441.

Using the Policy Filter Tool

NetScreen-Security Manager provides a Policy Filter tool to filter policy rules-based on one or more filter condition specified for rule attributes. One filter can contain several filter conditions for different attributes. The filter only applies to the current selected rulebase and does not affect other open devices. The filter results are displayed in the same rulebase. Rules that do not match filter conditions are hidden. In the firewall rulebase, only open rule groups are filtered. When a filter is set and a closed rule group is expanded, only rules that match the filter will be displayed in the group. For detailed information on how to use the Policy Filter tool, refer to the NetScreen-Security Manager Online Help.

Using a Security Policy Template

When you create a new Security Policy, you can select from the following options:

- Use the Default Security Policy—This policy contains the Zone rulebase with a single default firewall rule. Use this policy when creating firewall rules in the Zone, Global, and Multicast rulebases.
Use an existing Security Policy—a Security Policy copied from an existing policy is saved as the new policy. Use an existing policy when creating a policy that contains rulebases and rules that you want to modify for new security devices.

Use a Security Policy template—a template is a set of rules of a specific rulebase type that you can use as a starting point when creating a Security Policy. A Security Policy created from a template contains a set of predefined rulebases and rules. Because policy templates contains rules for the firewall and IDP rulebases, you might want to use a template when configuring rules for an ISG 2000 or ISG 1000 security device running ScreenOS 5.0.0-IDP1.

NetScreen-Security Manager includes the following Security Policy templates:

- all_with_logging. This template includes all Attack Objects and enable packet logging for all rules.
- all_without_logging. This template includes all Attack Objects but does not enable packet logging.
- Default. This template contains a good blend of security and performance.
- dmz_services. Use this template to protect a typical DMZ environment.
- dns_server. Use this template to protect DNS services.
- file_server. Use this template to protect file sharing services, such as SMB, NFS, FTP, and others.
- getting_started template. This template is designed to help you implement the IDP system and fine-tune the policy to your network. Use this template if you are new to intrusion detection configuration.
- inline_template. Use for IDP systems running in inline mode.
- network_scanner. Use this template to transparently gather information about your network.
- sniffer_template. Use for IDP systems running in inline tap mode.
- web_server. Use this template to protect HTTP servers from remote attacks.

Each Security Policy template contains rules that use the default actions associated with the Attack Object severity and protocol groups. You should customize these templates to work on your network by selecting your own Address Objects as the Destination IP and choosing IDP actions that reflect your security needs.

Filtering the Comment Field

You can use filters for the comments field of your policy. By default, search is an exact match unless used with a regular expression.
As an example, you have two rules with the following two comments: “test1” and “juniper;\test1”. If you want to find all the rules that have “test1” in the comments field, you must use a regular expression. If you do not use regular expression checkbox, the search returns rules with comment “test1” only.

In this example, if you want to find all rules that end with the string test1, use either of the following two regular expressions:

- .*test1.*\ntest1
- (.*|.*\n)test1

**Adding Rulebases**

When creating a Default Security Policy, only the Zone rulebase is added to the policy. You can add intrazone rules, VPN rules, and VPN links to this rulebase, but to add rules in other rulebases, you must first add that rulebase to the Security Policy.

To add a rulebase:

1. In the main navigation tree, select Security Policies, then double-click the policy name in the Security Policies window.

2. Click the Add icon in the upper right corner of the Security Policy window and select Add <name> Rulebase. The rulebase tab appears.

3. To configure a rule in the rulebase, click the Add icon on the left side of the Security Policy window. A default rule appears.

The following sections detail how to configure rules in each rulebase.

**Configuring Firewall Rules**

The firewall rulebases enable you to create zone and global firewall rules that control the flow of traffic on your network. You can configure the following settings for a firewall rule:

- Defining Match for Firewall Rules
- Defining Actions For Firewall Rules
- Selecting Devices for Firewall Rules
- Configuring Firewall Rule Options
- Comments For Firewall Rules

For each rule, you must configure the rule parameters for the Match columns. The remaining columns are optional, however, the more specific you can be in defining rule parameters in each column, the more efficient your Security Policy can be when protecting your network.
Defining Match for Firewall Rules

A firewall rulebase controls traffic flow on your network, from one network component to another network component. To do this, the firewall must know the path that the traffic takes to reach its destination and the service the traffic uses to get there.

When creating your firewall rules, you must specify the areas in your network that the traffic passes through. These areas include the network components that originate and receive the traffic, and the firewall zones the traffic passes through. For firewall rules:

- The Destination Address, Source Address, Service, and Action are required for all rules in the Zone and Global rulebases.
- The To Zone, From Zone, and service are required for rules in the Zone rulebase.

The following sections detail the Match columns of a firewall rule.

Configuring Source and Destination Zones for Firewall Rules

In the Zone rulebase, you create firewall rules to enable traffic to flow between zones (interzone) or between two interfaces bound to the same zone (intrazone). You must create zones on your security device before you can create a rule for that device. In a single rule:

- You must select a single zone for the source zone and a single zone for the destination zone. These zones must be available on the security devices you will install the policy on.
- You can also select multiple zone exceptions for both source and destination zones. A zone exception includes a specific zone and the device that contains that zone.
- You cannot create a rule that controls traffic between zones shared by vsys devices, or by devices in an NSRP configuration.

The Global rulebase does not contain source and destination zone columns. Because global rules permit or deny traffic flow between all zones on the security device, both the source and destination zones are global and so are not displayed.

Configuring Source and Destination Addresses For Firewall Rules

You create firewall rules to enable traffic to flow between two network components. In the NetScreen-Security Manager system, address objects are used to represent the components on your network: hosts, networks, and servers. When you add the address object to the rule, you are assigning it to a security zone on your security device.

You can add predefined Address Objects for the network components that originate and receive the traffic, or configure them as you create a firewall rule to control traffic between those components:

- To predefined an Address Object, see “Configuring Address Objects” on page 444.
To configure an Address Object as you are configuring the Source and Destination components of a rule, right-click in the Source or Destination column of a rule and select Add Address. Next, click the Add icon at the top of the New Source Addresses or New Destination Addresses dialog box and configure the desired address object. For details on configuring an address objects, see “Configuring Address Objects” on page 444.

You can also negate all address objects in the source or destination columns of a rule. When the source or destination is negated, NetScreen-Security Manager considers all address objects defined for the current domain except the negated objects as part of the source or destination for that rule. To negate the source or destination, you must have previously added one or more address objects to the source or destination column of a rule.

You can add a global MIP and or VIP objects as the source or destination address in a rule. However:

- When installing the rule on devices running ScreenOS 4.0, you can add multiple MIPs.
- When installing the rule on devices running ScreenOS 5.3, you can add multiple MIPs and VIPS.
- When installing the rule on devices running ScreenOS 5.0 or higher, you can add a single MIP object per rule. To use multiple MIP objects for these devices, you must use a separate rule for each global MIP object.

If you select multiple MIP or VIP objects in the source or destination column of a rule that includes devices running non-ScreenOS 5.3 or higher in the Install On column, a validation message appears, indicating that those devices do not support multiple MIPs or VIPS within a single rule.

EXAMPLE: SETTING INDIVIDUAL SOURCES AND DESTINATIONS IN RULES
To control incoming Internet traffic to your trusted network, set the From Zone to Untrust and the To Zone to Trust. Set the source address as any and the destination to the address object that represents your trusted network.

Your rule is similar to the example below:

**Figure 115: Set Individual Sources and Destinations in a Firewall Rule**

<table>
<thead>
<tr>
<th>Match</th>
<th>Source</th>
<th>To Zone</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>From Zone</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>untrust</td>
<td>any</td>
<td>trust</td>
<td>Internal Network only</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>any</td>
</tr>
</tbody>
</table>
To create a broader rule that controls traffic between multiple network components, create Address Object groups and use them in your firewall rules as you would other address objects. However, because security devices running ScreenOS 4.0.x apply firewall rules to each address object separately, using address object groups can quickly decrease the number of available internal logical rules. If you must use address groups for both the source and destination, ensure that these groups are as small and as specific as possible.

**EXAMPLE:** Setting Group Sources and Destinations in Rules
To control traffic from your Marketing servers to your Engineering Servers, set the To Zone to Engineering and the From Zone to Marketing. Set the source address as the address group object that represents your Marketing servers, and the destination address to the address group object that represents your Engineering servers.

Your rule is similar to the example below:

Figure 116: Set Group Sources and Destinations in a Firewall Rule

<table>
<thead>
<tr>
<th>Match</th>
<th>From Zone</th>
<th>Source</th>
<th>To Zone</th>
<th>Destination</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="Marketing" alt="Marketing" /></td>
<td><img src="Marketing" alt="Marketing" /></td>
<td><img src="Engineering" alt="Engineering" /></td>
<td><img src="Engineering" alt="Engineering" /></td>
<td>ANY</td>
<td>any</td>
</tr>
</tbody>
</table>

The more specific you are in defining the source and destination address in a firewall rule, the better your firewall performance.

**EXAMPLE:** Negating Sources in Rules
To permit incoming traffic to your Engineering department network from any network except the Sales network, set the From Zone to Untrust and the From Zone to Trust. Set the source address group as the address group that represents Outside Sales network, and the destination address to the address group that represents your Engineering server network. Finally, right-click inside the source address column for the rule and select Negate.

Your rule is similar to the example below:

Figure 117: Negate Source in a Firewall Rule

<table>
<thead>
<tr>
<th>Match</th>
<th>From Zone</th>
<th>Source</th>
<th>To Zone</th>
<th>Destination</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="untrust" alt="untrust" /></td>
<td><img src="Sales" alt="Sales" /></td>
<td><img src="trust" alt="trust" /></td>
<td><img src="Engineering" alt="Engineering" /></td>
<td>ANY</td>
<td>any</td>
</tr>
</tbody>
</table>

Add Address...

Negate Source
Configuring Services for Firewall Rules

Services are application layer protocols that define how data is structured as it travels across the network. In NetScreen-Security Manager, Service Objects represent the services running on your network. In a firewall rule, you specify which services are supported by the destination address object.

NOTE: All services rely on a transport layer protocol to transmit data. NetScreen-Security Manager includes services that use TCP, UDP, RPC, and ICMP transport layer protocols.

NetScreen-Security Manager comes with several service objects based on industry-standard services already created for you. You use these predefined service objects in firewall rules to specify the services that traffic can use to traverse your network.

EXAMPLE: SETTING STANDARD SERVICES IN RULES
To control FTP traffic from the Engineering Server in the trust zone to the corporate Web Server in the DMZ zone, select the FTP, HTTP, IMCP ANY, and TELNET service objects. Your rule is similar to the example below:

Figure 118: Set Standard Services in a Firewall Rule

You can create your own Service Objects to use in rules using the Object Editor, such as Service Objects for protocols that use non-standard ports.

EXAMPLE: SETTING CUSTOM SERVICES IN RULES
If you use a non-standard port (8080) for your HTTP services, create an HTTP Service Object on port 8080. Add this Service Object to your firewall rule. NetScreen-Security Manager uses the specified service object, HTTP on port 8080, and considers all connections to TCP/8080 to be HTTP connections. Your rule is similar to the example below:

Figure 119: Set Custom Services in a Firewall Rule
If the service of the network traffic matches a service selected in the rule, the firewall performs the action.

NOTE: For firewall rules installed on a ScreenOS 5.x device, if you use a custom service to relocate an application to a non-standard port, you must also enable the Application option in the Rule Options > Miscellaneous > ScreenOS 5.x devices. For details, see “ScreenOS 5.x Options” on page 547.

Defining Actions For Firewall Rules

You can specify the action that your security device performs against traffic that matches the zones, address objects, and services specified in the firewall rule. You can set different actions for each rule:

- Permit—The managed device permits the traffic to pass through the firewall to its destination address.
- Deny—The managed device does not permit the traffic to pass through the firewall, and drops all associated packets. No notification is returned to the sender.
- Reject—The managed device does not permit the traffic to pass through the firewall, and drops all associated packets. For TCP and UDP packets, the device returns a notification message to the packet sender:
  - When the device drops a TCP packet, it returns a TCP RST packet to the sender.
  - When the device drops a UDP packet, it returns an ICMP port unreachable error to the sender.

For non-TCP and non-UDP packets, no notification is returned to the sender.

When you permit traffic, you can also:

- Use logging to monitor suspicious or abnormal uses of permitted traffic (such as excessive Web surfing).
- Use AntiVirus to detect viruses in permitted traffic.
- Use URL Profiles to detect and prevent access to malicious or undesirable URLs.
- Use DI Profiles to detect and prevent attacks in permitted traffic.

Selecting Devices for Firewall Rules

In the install on column, select the device/s that receive and use this rule. You can select multiple security devices on which to install the firewall rule. After you have created the Security Policy and assigned it to a device, NetScreen-Security Manager installs the rule only on the devices specified in the Install Column of the rule, enabling you to use a single Security Policy for multiple security devices.
To see the exact rules that are applied to a specific device, in Device Manager, right-click a device and select Policy > View Pending Device Policy.

NOTE: If a device specified in the Install column does not support a specific rule option configured for the rule, you can still install the Security Policy on the device, but the rule option is not enabled for that device. Additionally, during policy validation, a warning appears for each unsupported rule option. For details, see “Validating Security Policies” on page 577.

Configuring Firewall Rule Options

Rule options enable you to configure additional protection mechanisms and other miscellaneous features. You can configure the following rule options:

- Enabling NAT
- Enabling GTP for Firewall Rules
- Configuring Traffic Shaping in a Security Policy
- Enabling Logging and Counting for Firewall Rules
- Miscellaneous
- ID
- Configuring WEB Filtering for Firewall Rules
- Configuring Authentication For Firewall Rules
- Configuring AntiVirus For Firewall Rules
- Configuring a DI Profile/Enable IDP For Firewall Rules

To quickly configure all rule options, right-click the Rule Options column and select Configure All Options. The Configure Options dialog box appears; select the option tab you want to configure for the rule.

Enabling NAT

You can configure policy-based network address translation (NAT) for a firewall rule. NAT enables the security device to translate the IP address of incoming or outgoing traffic so that the packets are routeable on the network.

Edit Source NAT

You can configure the security device to translate the source IP address:

- To translate the source IP address using a predefined range of IP addresses, select NAT and choose a Dynamic IP pool (DIP) object. For each matching packet, the device translates the original source address into a IP address selected from the DIP pool.
To translate the source IP address using the IP address of the outgoing interface on the security device, select Use Interface.

**Edit Destination NAT**

You can configure security devices running ScreenOS 5.x to translate the destination IP address. Enable Destination NAT and enter the destination IP address you want to translate to.

Other destination NAT options include:

- **Destination Port**—Your security devices can perform one-to-one destination NAT without changing the destination port numbers. However, you can configure the device to map the original destination port number in the segment header to another port number.

  - To enable destination port translation, select Destination Port and enter the port number you want to translate to.

  - To use the original destination port number, leave the default of None.

- **Upper IP Address**—Your device can also translate the destination IP address to a range of IP addresses. Select the Upper IP Address and enter the upper IP address. The device uses an address shifting mechanism to maintain the relationships among the original range of destination addresses after translating them to the new range of addresses.

Using Device Manager, you can also implement NAT on any device interface in any zone except Untrust. For details, see “Configuring Interface NAT” on page 230. For details on configuring NAT objects, see “Configuring NAT Objects” on page 516.

**Enabling GTP for Firewall Rules**

You can use a GTP object in a firewall rule to control how your security devices handle GPRS traffic. To add a GTP object, you must have already configured the object in Object Manager. For details, see “Configuring GTP Objects” on page 486.

**Configuring Traffic Shaping in a Security Policy**

Traffic shaping enables you to control the amount of bandwidth that is available to the matching network traffic in a rule. You can also define a priority that defines how the security device handles the matching network traffic that exceeds the defined maximum bandwidth. For security devices running ScreenOS 5.3, you can also manage the flow of traffic through the security device by limiting bandwidth at the point of ingress.

You can configure the following traffic shaping parameters:

- **Traffic Shaping Mode**—The traffic shaping mode is automatically determined by the security device, but you can set it to on or off.
Bandwidth—You can control the amount of bandwidth that is available to the matching network traffic. When traffic shaping is enabled, you can configure the minimum, or guaranteed bandwidth allowed, by setting the number of kilobits per second (kbps) using the Guaranteed Bandwidth field. This setting guarantees that this minimum amount of throughput is allowed to pass through the security device. In a similar manner, you can set the maximum bandwidth allowed using the Maximum Bandwidth field. For matching traffic that falls between the guaranteed and maximum settings, the security device passes traffic based on the priority setting.

NOTE: It is recommended that you do not set the maximum bandwidth to less than 10 kbps. Your security device might drop packets or the source address might attempt to resend the traffic repeatedly.

For security devices running ScreenOS 5.3, you can also manage the flow of traffic through the security device by limiting bandwidth at the point of ingress. To configure the maximum amount of traffic allowed at the interface ingress, you need to first enable Use Policing Bandwidth, and then set the number of kilobits per second (kbps) using the Policing Bandwidth field. This setting allows you to manage the maximum amount of traffic allowed to pass through the ingress interface.

Priority—You can set a priority for each firewall rule in your Security Policy. Your security device passes permitted traffic according to the priority level specified in the matching rule. The higher the priority level of the rule, the faster the matching traffic for that rule passes. You can configure the mappings of eight priority levels to the first three bits in the DiffServ field, or to the IP precedence field in the ToS byte in the IP packet header. By default, the highest priority (priority 0) on the security device maps to 111 in the IP precedence field. The lowest priority (priority 7) maps to 000 in the IP precedence field.

DSCP Class Selector—NetScreen-Security Manager uses the Differentiated Services Code Point (DSCP) mechanism to set priority levels. Using DSCP, you can mark traffic at a position within a hierarchy of priority. You can map eight priority levels to the DiffServ system: Priority 0 is the highest priority, and priority 7 is the lowest priority. Each priority level maps to a specific set of bits in the DiffServ field or the IP precedence field in the ToS byte of the IP packet header. The class selector controls the number of bits affected in the DiffServ field. By default, the priority levels affect only the first three bits in the eight bit DiffServ field. The remaining bits are untouched, but can be altered by an upstream router, which might change the IP priority preference.

When the DSCP class selector is enabled, the class selector zeroes the remaining five bits in the DiffServ field, which prevents upstream routers from altering priority levels.

For details on changing the default mappings between priority levels and the DiffServ system, see “Configuring Traffic Shaping” on page 334.

NOTE: You can only apply traffic shaping to rules whose destination zone has a single interface bound to it. Security zones that contain subinterfaces or that contain more than one physical interface do not support traffic shaping.
For more details on Traffic Shaping, refer to the NetScreen Concepts & Examples ScreenOS Reference Guide.

Enabling Logging and Counting for Firewall Rules

A good Security Policy generates enough log entries to fully document only the important security events on your network. However, if you need to keep a record of all log entries for archiving and accountability, you can design your rule to log every security event. For critical events, you might even want to be notified immediately by email or set an alert to appear in the log entry.

Log entries appear in real-time in the Log Viewer, and are also used in the Log Investigator for cross-tabulation of security events. Your goal is to fine-tune the notifications in your Security Policy to your individual security needs.

Configuring Logging and Alerts

To log an event for a rule, enable logging. Each time your security device matches network traffic to the rule, the device creates a traffic log entry that describes that event and NetScreen-Security Manager displays the traffic log entry in the Log Viewer. You can enable logging when a session is initialized, closed or both on a security device. For a list of possible traffic log entries, see “Traffic Log Entries” on page 901.

Depending on your security needs, you might want NetScreen-Security Manager to provide additional notification when a rule is matched, such as an alert in the log entry. An alert is a notification icon ( ) that appears in a log entry in the Log Viewer. When you enable alerts in your firewall rule and traffic matches that rule, the device generates a traffic log entry that includes an alert. Alerts can help you quickly identify specific network traffic, such as critical severity attacks.

You must enable logging before you can enable alerts.

Configuring Counting and Alarms

Counting and alarms work together to help you track the amount of traffic that is matching your firewall rule. Counting enables the device to count the number of bytes in network traffic that matches the firewall rule. Using this data, the device can then generate alarms that notify you when the matching network traffic falls outside your predefined byte range.

To set an alarm, enable counting and specify the minimum and maximum byte thresholds for matching network traffic. You can specify a predefined number of bytes per second, number of Kilobytes per minute, or both. Each time your security device detects network traffic that exceeds the alarm threshold in the rule, the device generates an alarm log entry for that describes that event and displays it in the Log Viewer. For a list of possible alarm log entries, see “Alarm Log Entries” on page 833.

You must enable counting before you can enable alarms. Although you can enable counting without also enabling alarms, NetScreen-Security Manager does not use the counting data except to trigger alarms. If you do not intend to use alarms, you should leave counting disabled. Additionally, because counting can impact performance during heavy traffic periods, you should enable counting and alarms only for firewall rules that detect important activity.
Configuring Log Actions

Use the Log Actions tab that appears when you select Log/Count in the Rule Options column to configure the following actions to occur when a log is generated from a specific rule:

- **Sending SNMP Trap**—Selecting this option directs the system to output logs to an SNMP server in SNMP format.
- **Sending Syslog Messages**—Selecting this option directs the system to output logs to a syslog server in syslog format.
- **Writing CSV files**—Selecting this option and specifying a filename directs the system to output logs using in CSV format.
- **Writing XML Files**—Selecting this option and specifying a filename directs the system to output logs using XML.
- **Sending Email**—Selecting this option directs the system to output logs to an email address in SMTP format. You must specify the recipient email address(es) that receives the exported log records.
- **Running Scripts**—Selecting this option directs the system to execute a script, and report output status. You must specify the script that receives the exported log records (script must be located in the /usr/netscreen/DevSvr/var/scripts/ directory). In the event that the script fails, you can also configure the system to retry or skip running the script again.

You can configure parameters for forwarding logs to SNMP, Syslog, Email, CSV and XML in the Action Parameters node of the Action Manager.

NOTE: You can configure log actions to occur for all rulebases that include logging options (i.e., IDP rulebase, Backdoor rulebase).

Miscellaneous

The following sections detail the Miscellaneous rule options.

Schedule

To control the time period that your security device applies the rule to your network traffic, you can define a schedule for the rule. If you define a schedule, the security device applies the rule to your network traffic only during the time period specified in the schedule; if you do not specify a schedule, the rule is always applied to your network traffic.

In NetScreen-Security Manager, schedules are represented by Schedule Objects. Before you can define a schedule for rule, you must create a Schedule Object that describes a time period. The Schedule Object details the start time and date, end time and date, and frequency (recurring or one-time) of the time period. For more details on creating Schedule Objects, see “Configuring Schedule Objects” on page 448.

You can use schedules to control the flow of network traffic at a time-sensitive level, and also enhance your network security.
EXAMPLE: SETTING SCHEDULE OBJECTS IN RULES
To prevent employees from downloading large files during business hours, set the Service Object to FTP, the Action to deny, and configure traffic shaping to limit bandwidth. Using the Object Manager, create a Schedule Object called Business Day that describes the time period of 9:00am to 7:00pm, M-F, recurring weekly. Right-click the schedule column in the rule and select the Business Day schedule object.

HA Session Backup
NetScreen-5XT and NetScreen-5GT security devices can disable active firewall rules that permit traffic if the session switches over to the modem link. This feature is ON by default.

ScreenOS 5.x Options
For security devices running ScreenOS 5.x, you can configure additional rule options.

- Application—You can configure the security device to handle the service for the firewall rule as a known Layer 4 protocol service. If you are using application relocation (using a nonstandard port to handle an application service), enable this option to ensure that the security device correctly checks traffic.

ID
The rule ID is a number that uniquely identifies a rule within the rulebase and Security Policy. After you install a rule as part of a Security Policy on a security device, you can view this rule by logging in locally to the device. However, when viewed through the WebUI or CLI, the rule appears as an individual policy. The individual policy on the device has the same ID as the rule in the management system, which helps you keep track of which rules are on which devices.

You can configure a rule ID for any Zone-based firewall rule or VPN rule:

- For new rules, NetScreen-Security Manager automatically assigns a unique ID to that rule. You can change this ID, if desired, or leave the ID number.

- For rules that are already installed on a device, NetScreen-Security Manager has already created a unique ID for the rule. You can change this predefined ID if desired, to an ID number, or leave the ID set to “none”, which preserves the autogenerated ID number.

NOTE: When the ID is set to “none”, NetScreen-Security Manager uses a hashing algorithm on the source zone, destination zone, source address, destination address, and service fields for the rule to generate a unique ID.

- For VPN rules that are automatically created by VPN Manager, NetScreen-Security Manager creates a unique ID for each VPN rule. You can change this predefined ID, if desired, to a ID number, or leave the predefined ID set to “none”, which preserves the autogenerated ID number.

When you copy and paste a rule within a rulebase, NetScreen-Security Manager automatically creates a new unique ID for the pasted rule.
You are not required to set a ID for a rule.

Configuring WEB Filtering for Firewall Rules

After you create a WEB Filtering profile (refer to Chapter 7, Configuring WEB Filtering (Integrated), and you have enabled WEB Filtering on your device (refer to Chapter 4, Configuring Devices), you need to bind it to your firewall rule. You need to select one of the following options:

- WEB Filtering Through SurfControl SCFP/WebSense (Redirect)—With this option, the security devices sends the first HTTP request in a TCP connection to either a Websense server or a SurfControl server, enabling you to block or permit access to different web sites based on their URLs, domain names, and IP addresses.

- WEB Filtering Through SurfControl CPA (Integrated)—With this option you permit or block access to a requested website by binding the default ns-profile or custom profile you created to a firewall rule.

When a profile is bound to the firewall rule, the security device matches the URL in the incoming HTTP request to the categories in the profile in the following sequence:

- Black List
- White List
- Custom URL Lists
- Predefined URL Categories

If no custom profile is bound to the firewall rule, the security device uses the default profile ns-profile. If the security device does not find the category of the requested URL, then it performs the default action, to permit access to the URL (unless otherwise configured).

EXAMPLE: SETTING A WEB FILTERING PROFILE IN A RULE

In this example, you will bind the predefined WEB Filtering profile to a firewall rule.

1. Click Security Policies in the navigation tree. Select the device you want to bind to the URL filter profile.

2. In the Zone based Firewall Rules main display area, right-click under Rule Options. A pull-down menu appears.

3. Select WEB Filtering.
4. In the Edit URL Filter dialog box, click Enable.


6. Select the custom profile, New_Block_List, to bind to the firewall rule.

   **NOTE:** You can only bind one WEB Filtering profile to a firewall rule.

7. Click OK.
Configuring Authentication For Firewall Rules

You can authenticate the identity of the user who is generating the network traffic. When you enable authentication in the rule, the user must authenticate future network traffic by supplying a user name and password in an initial, separate HTTP, FTP, or Telnet connection. If the user fails to authenticate using one of these services or provides incorrect credentials, the authentication requirement for the rule is not met and the network traffic is denied. (Typically, when you enable authentication, you also use the permit action.)

NOTE: You cannot enable authentication for a rule that includes the DNS/53 Service Object.

Configuring Authentication

Authentication enables you to control which RAS users can connect to the protected network and how they can connect. When you select an authentication server, you must also configure the users that authentication server authenticates.

Select the authentication mechanism:

- No Authentication—Use this option to enable the specified RAS users to connect without authentication.
- Authentication—Use for RAS users that use HTTP, FTP, or Telnet services to connect to the protected network.
- Web Authentication—Use for RAS users using HTTP to connect to the protected network.
- Infranet Authentication—Use this option to enable specified RAS users to connect using a Juniper Networks Infranet Controller.

Configuring Users

RAS users are represented by User Objects. Before you can authenticate a user in a firewall rule, you must create a User Object that defines the user name, user password, and the authentication location (local or external). For Authentication and Web Authentication, configure the users:

- User—Select the User object that represents the user you want to authenticate.
- User Group—Select the User Group object that represents the users you want to authenticate.
- Group Expression—Select the Group Expression object.
- Allow Any—Use this option to authenticate any user or user group.

To authenticate RAS users with Authentication, you must include HTTP, FTP, or Telnet service objects in the Service column of the rule. You can include other services as well, or select any to specify all services. To make a connection to the destination IP address in the rule, the RAS user first initiates an HTTP, FTP, or Telnet connection to the destination address; the security device intercepts the request packet and responds with a login prompt for user credentials.
Chapter 9: Configuring Security Policies

- If the destination address is a subnet, the remote user must authenticate for each IP address in that subnet.

- If the source address supports multiple remote user accounts (such as a Unix host running Telnet) OR is located behind a NAT device that uses a single IP address for all NAT assignments, only the first remote user from that source address must initiate and authenticate an HTTP, FTP, or Telnet connection. All subsequent remote users from that source address do not need to authenticate, and can pass matching network traffic to the destination address.

To authentication RAS users with Web Authentication, you must include HTTP service object in the Service column of the rule. To make a connection to the destination address in the rule, the RAS user first initiates an HTTP connection to the Web Authentication server. The security device responds with a login prompt for user credentials.

For more details on User Objects, see “Configuring User Objects” on page 507.

Configuring AntiVirus For Firewall Rules
To configure AntiVirus protection for a firewall rule:

- None—No AntiVirus protection enabled.
- Use External AV Server—Uses an external antivirus scanner. Select an external policy object that defines an external scanner.
- Use Scan Manager—Scan Manager is an embedded scanning engine. To use Scan Manager, the security device you install the policy on must be a NetScreen-5GT or NetScreen-Hardware Security Client device running ScreenOS 5.0 - 5.2. If you install a policy that uses Scan Manager on a different device, the device executes and processes traffic according to the rule, but does not detect viruses using the embedded scanning engine.
- Use Scan Manager with Profile—Scan Manager is an embedded scanning engine. This setting tells the device to use the global profile specified. This setting only works for devices running ScreenOS 5.3.

Configuring a DI Profile/Enable IDP For Firewall Rules
Use the DI Profile/Enable IDP rule options to configure Deep Inspection (DI) or Intrusion Detection and Prevention (IDP) functionality within the rule.

NOTE: DI and IDP are mutually exclusive. When you install the IDP license key on a security device, DI is automatically disabled.

Configuring DI Profile for a Rule
Security devices running ScreenOS 5.x include Deep Inspection attack protection that can detect malicious network traffic at the application level. To configure attack protection, select a DI Profile object in your firewall rule to detect intrusion attempts within permitted traffic.
Attacks are specific patterns of malicious activity within a network connection, and an attack object uses selected sections of the attack pattern to detect the attack itself. NetScreen-Security Manager contains a database of predefined attack objects that detect known and unknown attacks against your network. You can use these predefined attack objects (and your own custom attack objects) to create a DI Profile object, which you then use in a firewall rule. When configuring a DI Profile, you can also define the action that the device performs against those attacks when detected in permitted traffic. For details on creating a DI Profile object, see “Creating DI Profiles” on page 451.

You can configure one DI Profile for each rule. When the device detects a match between the permitted network traffic and an attack object within the selected DI Profile, the device generates an attack log entry.

To use a DI Profile:

- The firewall action must be permit. You cannot detect attacks in traffic that the device denies or rejects.
- The security device you install the policy on must be running ScreenOS 5.x. If you install a policy that contains a DI Profile on a ScreenOS 4.0.x device, the device executes and processes traffic according to the rule, but does not detect application-level attacks.

For a list of possible attack log entries, see “Deep Inspection Alarm Log Entries” on page 834.

**Configure IDP for a Firewall Rule**

When configuring rule for an IDP-capable device, such as the ISG 2000 or ISG 1000 security device running ScreenOS 5.0IDP1, you can enable IDP and select an IDP mode in the DI Profile/Enable IDP rule options. Enabling IDP directs the security device to pass all traffic permitted by the firewall rule to the IDP rulebase.

**NOTE:** DI and IDP are mutually exclusive. When you install the IDP license key on a security device, DI is automatically disabled.

When configuring the firewall rule, consider the following:

- Traffic that is denied by a firewall rule cannot be passed to IDP rules. To enable IDP in a firewall rule, the action must be permit.
- For firewall rules that pass traffic to the IDP rulebases, the Install On column must include IDP-capable devices only.

To forward traffic to the IDP rulebases, enable IDP and select one of the following modes:

- In inline mode, IDP is directly in the path of traffic on your network and can detect and block attacks. For example, you can deploy the ISG 2000 or ISG 1000 with integrated FW/VPN/IDP capabilities between the Internet and an enterprise LAN, WAN, or special zones such as DMZ.
In inline tap mode, IDP can detect attacks and provide notification. IDP receives a copy of a packet while the original packet is forwarded on the network. IDP examines the copy of the packet and flags any potential problems. IDP’s inspection of packets does not affect the forwarding of the packet on the network.

NOTE: You must deploy the ISG 2000 or ISG 1000 device inline. You cannot connect a device that is in inline tap mode to an external TAP or SPAN port on a switch.

Selecting either mode enables IDP for the firewall rule, and configures the security device to forward all permitted traffic to the IDP rulebases for further processing.

Comments For Firewall Rules

The Comments column of a rule contains the rule title, which is also the ScreenOS policy name (the name of the policy when viewing the device configuration using the WebUI).

You can also enter comments in the Comment Field, if desired.

Configuring Multicast Rules

A multicast rule is a statement that defines a specific type of multicast control traffic. When multicast control traffic passes through a security device, the device attempts to match that traffic against its list of rules. If a rule is matched, the device permits the traffic to pass through.

On security devices, you secure multicast control traffic using access lists. First, you create an access list, which defines one of the following:

- The multicast groups a host can join.
- The sources from which traffic can be received.

After creating an access list, you reference these access lists in a multicast rule in the Security Policy for the device.

Configuring Source and Destination Zones

In the Multicast rulebase, you create rules to enable multicast control traffic to flow between zones. You must create zones on your security device before you can create a rule for that device. In a single rule:

- You must select a single zone for the source zone and a single zone for the destination zone. These zones must be available on the security devices on which you install the policy.
- You can also select multiple zone exceptions for both source and destination zones. A zone exception includes a specific zone and the device that contains that zone.
Configuring Source and Destination Groups

When you create a multicast rule, specify the multicast groups for which you want to permit multicast traffic using one of the following methods:

- Specify a multicast group IP address, and optionally, the multicast group address on the outgoing interface
- Specify the access list that identifies the permitted multicast groups
- Select “any” to accept traffic for all multicast groups

Configuring Rule Options

Rule options enable you to specify the type of multicast control traffic to which this rule applies and whether the rule is bidirectional.

A rule can apply to either IGMP messages or PIM-SM messages:

- When running IGMP proxy on the security device, configure a rule that permits IGMP messages to flow between zones.
- When running PIM-SIM on the security device, configure a rule that permits PIM-SM messages.

EXAMPLE: CREATING A MULTICAST RULE

In this example, you define a multicast rule that permits IGMP messages from the Trust zone to the Untrust zone. You specify the original multicast group address object and a different destination multicast group object.

1. In the main navigation tree, select Object Manager > Address Objects.

2. In the main display area, click the Add icon and select Multicast Group. In the New Multicast Group dialog box, configure the following then click OK:

   - For Name, enter mcast1.
   - For Color, select green.
   - For IP Address, enter 232.1.1.1.
   - For Netmask, enter 32.

3. In the main display area, click the Add icon and select Multicast Group. In the New Multicast Group dialog box, configure the following then click OK:

   - For Name, enter mcast2.
   - For Color, select red.
   - For IP Address, enter 232.1.1.2.
   - For Netmask, enter 32.
4. In the main navigation tree, select Security Policies, then create a new multicast rule in the Multicast rulebase of a new or existing Security Policy.

5. Right-click in the Source Group column and select Configure Source/Destination. Configure as shown below:

Figure 122: Configure Source/ Destination for Multicast Rule

**Configuring Antivirus Rules**

Antivirus settings are stored in a profile. To see how to create an antivirus profile, see Configuring AntiVirus Objects on page 478.

To assign an antivirus profile to a policy, do the following:

1. Double-click the Rule Options cell in a rule.
2. In the Configure Options dialog, click the Antivirus tab.
3. Select an Antivirus option:
   - None—Turns off antivirus scanning for that rule.
   - Use External AV Server—Indicates that you want to use an External AV Server. You must select the external AV server you wish to use. To configure external AV servers, see Configuring External AV Profiles on page 478.
   - Use Scan Manager—Tells the device to use the settings on the device, instead of a profile. Necessary for ScreenOS 5.0-5.2.
   - Use Scan Manager with Profile—Tells the device to use the indicated antivirus profile. Necessary for ScreenOS 5.3 and higher. To set up an internal antivirus profile, see Configuring Internal AV Profiles on page 479.
4. Click OK.
Configuring Antispam Rules

Antispam settings are stored in profiles. Initially, Netscreen-Security Manager will have only one antispam profile available: ns-profile.

To assign an antispam profile to a policy, do the following:

1. Double-click the Rule Options cell in a rule.
2. In the Configure Options dialog, click the Antispam tab.
3. Check the Enable Antispam profile checkbox.
4. Select ns-profile in the Profile Name pull-down menu.
5. Click OK.

Configuring IDP Rules

The IDP rulebase protects your network from attacks by using attack objects to identify malicious activity and take action. Creating an IDP rule involves the following steps:

- Defining Match for Firewall Rules—The type of network traffic you want IDP to monitor for attacks, such as source/destination zones, source/destination address objects, and the application layer protocols (services) supported by the destination address object. You can also negate zones, address objects, or services.

- Configuring Terminal IDP Rules—By default, rules in the IDP rulebase are non-terminal, meaning that IDP examines all rules in the rulebase and all matches are executed. You can specify that a rule is terminal; if IDP encounters a match for the source, destination, and service specified in a terminal rule, it does not examine any subsequent rules for that connection. Note that the traffic does not need to match the attacks specified in the terminal rule. Terminal rules should appear near the top of the rulebase, before other rules that would match the same traffic. Use caution when specifying terminal rules.

- Configuring Attack Objects in IDP Rules—The attacks you want IDP to match in the monitored network traffic. Each attack is defined as an attack object, which represents a known pattern of attack. Whenever this known pattern of attack is encountered in the monitored network traffic, the attack object is matched. You can add attack objects by category, operating system, severity, or individually.

- Configuring Actions—The action you want IDP to take when the monitored traffic matches the rule’s attack objects. You can specify the action you want the security device to perform against the current connection (see “Defining Actions For IDP Rules” on page 562) and future connections from the same source IP address (see “Choosing an IP Action” on page 565).

- Configuring Notification in IDP Rules—Disable or enable logging for the IDP rule.

The following sections detail each step.
Defining Match For IDP Rules

When creating your IDP rules, you must specify the type of network traffic that you want IDP to monitor for attacks. These characteristics include the network components that originate and receive the traffic, and the firewall zones the traffic passes through.

The Match columns From Zone, Source, To Zone, Destination, and Service are required for all rules in the IDP rulebase. The Terminate Match selection allows you to designate a rule as terminal; if IDP encounters a match for the other Match columns in a terminal rule, no other rules in the rulebase are examined. The matching traffic does not need to match the attacks specified in a terminal rule. (For more information on terminal rules, see “Configuring Terminal IDP Rules” on page 561.

The following sections detail the Match columns of an IDP rule.

Configuring Source & Destination Zones for IDP Rules

You can select multiple zones for the source and destination, however these zones must be available on the security devices on which you will install the policy. You can specify “any” for the source or destination zones to monitor network traffic originating or destined for any zone.

NOTE: You can create custom zones for some security devices. The list of zones from which you can select source and destination zones includes the predefined and custom zones that have been configured for all devices managed by NetScreen-Security Manager. Therefore, you should only select zones that are applicable for the device on which you will install the Security Policy.

Configuring Source & Destination Address Objects for IDP Rules

In the NetScreen-Security Manager system, address objects are used to represent components on your network: hosts, networks, servers, etc. Typically, a server or other device on your network is the destination IP for incoming attacks, and can sometimes be the source IP for interactive attacks (see “Configuring Backdoor Rules” on page 572 for more information on interactive attacks). You can specify “any” to monitor network traffic originating from any IP address. You can also “negate” the address object(s) listed in the Source or Destination column to specify all sources or destinations except the excluded object(s).

You can create address objects either before you create an IDP rule or while creating or editing an IDP rule. To select or configure an address object, right-click either the Source or Destination column of a rule and select Select Address. In the Select Source Addresses dialog box, you can either select an already-created address object or click the Add icon to create a new host, network, or group object.

EXAMPLE: SETTING SOURCE AND DESTINATION

You want to detect incoming attacks that target your internal network. Set the From Zone to Untrust and the Source IP to any. Set the To Zone to dmz and trust. Select the address object that represents the host or server you want to protect from attacks as the Destination IP. Your rule looks similar to this example:
Configuring IDP Rules

EXAMPLE: SETTING MULTIPLE SOURCES AND DESTINATIONS
You want to detect attacks between two networks. Select multiple address objects for the Source and Destination. Your rule looks similar to this example:

Figure 124: Set Multiple Source and Destination Networks

The more specific you are in defining the source and destination of an attack, the more you reduce false positives.

Configuring Services for IDP Rules

Services are application layer protocols that define how data is structured as it travels across the network. Because the services you support on your network are the same services that attackers must use to attack your network, you can specify which services are supported by the destination IP to make your rule more efficient.

Service objects represent the services running on your network. NetScreen-Security Manager includes predefined service objects that are based on industry-standard services. You use these service objects in rules to specify the service an attack uses to access your network. You can also create custom service objects to represent protocols that are not included in the predefined services. For more information about configuring service objects, see “Configuring Service Objects” on page 492.

In the Service column you select the service of the traffic you want IDP to match:

- Select Default to accept the service specified by the attack object you select in the Attacks column. When you select an attack object in the Attack column, the service associated with that attack object becomes the default service for the rule. To see the exact service, view the attack object details.
- Select Any to set any service.

NOTE: All services rely on a transport layer protocol to transmit data. IDP includes services that use TCP, UDP, RPC, and ICMP transport layer protocols.
Select Service to choose specific services from the list of defined service objects.

**EXAMPLE: SETTING DEFAULT SERVICES**
You want to protect your FTP server from FTP attacks. Set the service to Default, and add an attack object that detects FTP buffer overflow attempts. The Service column in the rule still displays “Default”, but the rule actually uses the default service of TCP-FTP, which is specified in the attack object. Your rule looks similar to this example:

Figure 125: Set Default Services

<table>
<thead>
<tr>
<th>From Zone</th>
<th>Source</th>
<th>To Zone</th>
<th>Destination</th>
<th>Service</th>
<th>Terminate Match</th>
<th>Action</th>
<th>Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>untrust</td>
<td>any</td>
<td>dmz</td>
<td>FTP Server</td>
<td>Default</td>
<td>☑</td>
<td>☑</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td></td>
<td>trust</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>FTP - Critical</td>
</tr>
</tbody>
</table>

**EXAMPLE: SETTING CUSTOM SERVICES**
Your mail server supports POP3 and SMTP connections but not IMAP. Set POP3 and SMTP service objects as services that can be used to attack that server. Because IMAP is not supported, you do not need to add the IMAP service object.

Your rule looks similar to the example below:

Figure 126: Set Custom Services

<table>
<thead>
<tr>
<th>From Zone</th>
<th>Source</th>
<th>To Zone</th>
<th>Destination</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>untrust</td>
<td>any</td>
<td>dmz</td>
<td>Web Server</td>
<td>SMTP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>trust</td>
<td></td>
<td>POP3</td>
</tr>
</tbody>
</table>

If you are supporting services on non-standard ports, you should choose a service other than default.

**EXAMPLE: SETTING NON-STANDARD SERVICES**
You use a non-standard port (8080) for your HTTP services. Use the Object Manager to create a custom service object on port 8080.
Figure 127: Add Non-Standard Services Object

Add this service object to your rule, then add several HTTP attack objects, which have a default service of TCP/80. IDP uses the specified service, HTTP-8080, instead of the default, and looks for matches to the HTTP attacks in TCP traffic on port 8080.

Your rule looks similar to this example:

<table>
<thead>
<tr>
<th>Match</th>
</tr>
</thead>
<tbody>
<tr>
<td>From Zone</td>
</tr>
<tr>
<td>untrust</td>
</tr>
</tbody>
</table>

Figure 128: Set Non-Standard Service

You can create your own service objects to use in rules, such as service objects for protocols that use non-standard ports. However, you cannot match attack objects to protocols they do not use.
Configuring Terminal IDP Rules

The normal IDP rule-matching algorithm starts from the top of the rulebase and checks traffic against all rules in the rulebase that match the source, destination, and service. A terminal rule is an exception to this normal rule-matching algorithm. When a match is discovered in a terminal rule for the source, destination, and service, IDP does not continue to check subsequent rules for the same source, destination, and service. It does not matter whether or not the traffic matches the attack objects in the matching rule.

You can use a terminal rule for the following purposes:

- To set different actions for different attacks for the same Source and Destination. This is illustrated by rules 3 and 6 in the “Setting Terminal Rules” example below.
- To disregard traffic that originates from a known trusted Source. Typically the action is None for this type of terminal rule. This is illustrated by rule 1 in the “Setting Terminal Rules” example below.
- To disregard traffic that is sent to a server that is only vulnerable to a specific set of attacks. Typically, the action is Drop Connection for this type of terminal rule.

Use caution when defining terminal rules. You can inadvertently leave your network open to attacks by creating an inappropriate terminal rule. Remember that traffic matching the source, destination, and service of a terminal rule is not compared to subsequent rules, even if the traffic does not match an attack object in the terminal rule. Use a terminal rule only when you want to examine a certain type of traffic for one specific set of attack objects and no others. Be particularly careful about terminal rules using “any” for both the source and destination.

Terminal rules should appear near the top of the rulebase, before other rules that would match the same traffic. You set a rule as terminal by selecting the box in the Terminate Match column of the Security Policy window when the rule is created or modified.

NOTE: In many cases, you can use an exempt rule instead of a terminal rule. You might find it easier and more straightforward to configure an exempt rule than a terminal rule. See “Configuring Exempt Rules” on page 568.

EXAMPLE: SETTING TERMINAL RULES

In the example IDP rulebase shown below, rules 1, 3, 4, and 5 are configured as terminal rules:

- Rule 1 terminates the match algorithm if the source IP of the traffic originates from the Security Network, a known trusted network. If this rule is matched, IDP disregards traffic from the Security Network and does not continue monitoring the session for malicious data.
- Rules 3 and 6 set different actions for different attacks when the destination IP is the Corporate or Europe E-mail server. Rule 3 terminates the match algorithm when the attack is an email that uses the SMTP context Confidential. Rule 6 closes the server when the attack is an SMTP attack.
Rule 4 terminates the match algorithm when the destination is the Web Server and the attack is a Critical or High HTTP attack. The rule ensures that IDP drops the most important HTTP attacks against the Web Server and does not continue to match the connection.

Rule 5 terminates the match algorithm when the source is the Internal Network and the attack is a Critical, High, or Medium Trojan Backdoor. The rule ensures that IDP closes both the client and server and does not continue to match the connection.

Figure 129: Set Terminal Rules

Defining Actions For IDP Rules

You can tell the security device which actions to perform against attacks that match rules in your Security Policy. For each attack that matches a rule, you can choose to ignore, drop, or close the current attacking packets or connection. If the rule is triggered, the device can perform actions against the connection.

Remember that the device can drop traffic only when IDP is enabled in inline mode; when IDP is enabled in inline tap mode, it cannot perform drop or close actions.

You can specify the following actions for IDP rules:

Table 30: IDP Rule Actions

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>IDP takes no action against the connection. If a rule that contains an action of None is matched, the corresponding log record displays “accept” in the action column of the Log Viewer.</td>
</tr>
<tr>
<td>Ignore</td>
<td>IDP ignores the remainder of a connection after an attack object in an IDP rule is matched.</td>
</tr>
</tbody>
</table>
### Configuring Attack Objects in IDP Rules

Attack objects represent specific patterns of malicious activity within a connection, and are a method for detecting attacks. Each attack object detects a known or unknown attack that can be used to compromise your network. For more information about attack objects, see “Working with IDP Attack Objects” on page 453.

To add attack objects to a rule, right-click the Attacks column of the rule and select Select Attacks. In the Add Attacks dialog box, you can add attacks using one or both of the following options:

- **Attack List**—Select this option to add individual attack objects from an alphabetically list of all predefined and custom attack objects. Attack objects are listed alphabetically by name of attack.

  Selecting individual attacks is a good option if you know the exact name of the attack you want to add to a rule. To locate a specific word or string in the attack object name, use the integrated search function in NetScreen-Security Manager; for details, see “Searching in the User Interface” on page 24.

- **Attack Groups**—Select this option to add attack object groups from three predefined dynamic attack groups (Category, OS, Severity); if you have created a custom dynamic group, that group is also listed.

  Selecting attack groups is a good option when you are unsure of the exact attack you want to add to a rule, but you know the type of attack protection you want the security device to provide. Within the Attack Groups, you can:

  - **Add all Attack Objects** (select All Attacks). Consider carefully before select this option; using all attack objects in a rule can severely impact performance on the security device.
  
  - **Add one or more attack groups** (hold down CTL to select multiple groups). Predefined dynamic groups might contain subgroups as well.
  
  - **Add individual attack objects** (hold down CTL to select multiple objects)

#### Action | Description
--- | ---
Drop Packet | IDP drops a matching packet before it can reach its destination but does not close the connection. Use this action to drop packets for attacks in traffic that is prone to spoofing, such as UDP traffic. Dropping a connection for such traffic could result in a denial of service that prevents you from receiving traffic from a legitimate source IP address.

Drop Connection | IDP drops the connection without sending a RST packet to the sender, preventing the traffic from reaching its destination. Use this action to drop connections for traffic that is not prone to spoofing.

Close Client and Server | IDP closes the connection and sends a RST packet to both the client and the server. If IDP is operating in inline tap mode, IDP sends a RST packet to both the client and server but does NOT close the connection.

Close Client | IDP closes the connection to the client, but not to the server.

Close Server | IDP closes the connection to the server, but not to the client.
The following sections detail each predefined dynamic attack group.

**Adding IDP Attack Object Groups by Category**

The Category group includes attack objects organized by services. Services are application layer protocols that define how data is structured as it travels across the network. A protocol is a specification that indicates how communication between two entities (applications, servers, Ethernet cards, etc.) occurs.

When attacking a system, attackers use the protocol of a supported service to communicate their malicious activity to the server. However, attackers can only use protocols that are supported by the system they are attacking. You can add a category group to the Attacks column in your rule; however, you need to select only the categories that are used by the address objects you are protecting with the rule.

For example, if you rely extensively on FTP and HTTP for file transfers to and from your Web servers, choose the FTP and HTTP category groups to carefully monitor all traffic that uses these services.

**Adding IDP Attack Objects by Operating System**

The Operating System group includes attack objects for several predefined operating systems to help you choose the attack objects that are the most dangerous to specific components on your network. You can choose BSD, Linux, Solaris, or Windows.

**Adding IDP Attack Objects by Severity**

The Severity group includes five attack object groups organized by severity level. You can select one or more groups to include in your rule. To protect critical address objects or “popular” attacker targets, such as your mail server, use multiple severity levels to ensure maximum protection.

We recommend using the following actions and notification settings when using severity-based dynamic attack groups in a rule:

<table>
<thead>
<tr>
<th>Severity</th>
<th>Description</th>
<th>Rec. Action</th>
<th>Rec. Notification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>Attacks attempt to evade an IDS, crash a machine, or gain system-level privileges.</td>
<td>Drop Packet, Drop Connection</td>
<td>Logging, Alert</td>
</tr>
<tr>
<td>Major</td>
<td>Attacks attempt to crash a service, perform a denial-of-service, install or use a Trojan, or gain user-level access to a host.</td>
<td>Drop Packet, Drop Connection</td>
<td>Logging, Alert</td>
</tr>
<tr>
<td>Minor</td>
<td>Attacks attempt to obtain critical information through directory traversal or information leaks.</td>
<td>(no recommended action)</td>
<td>Logging</td>
</tr>
<tr>
<td>Warning</td>
<td>Attacks attempt to obtain non-critical information or scan the network with a scanning tool. They can also be obsolete attacks or anomalous (but probably harmless) traffic.</td>
<td>(no recommended action)</td>
<td>Logging</td>
</tr>
<tr>
<td>Info</td>
<td>Attacks are normal, harmless traffic containing URLs, DNS lookup failures, and SNMP public community strings. You can use informational attack objects to obtain information about your network.</td>
<td>(no recommended action)</td>
<td>(no recommended notification)</td>
</tr>
</tbody>
</table>
You configure actions in the Action column of the rule; see “Defining Actions For IDP Rules” on page 562. You configure notification settings in the Notification column of the rule; see “Configuring Notification in IDP Rules” on page 566.

Adding Custom Dynamic Attack Groups
You can add previously-created custom dynamic attack groups to a rule.

Additionally, after you have added the custom group to a rule, you can edit the settings for the dynamic group by double-clicking the group icon in the rule.

Configuring IP Actions in IDP Rules
(This column only appears when you view the Security Policy in Expanded Mode. To change the Security Policy view from Compact Mode to Expanded Mode, from the menu bar, select View > Expanded Mode.)

If the current network traffic matches a rule, the security device can perform an IP action against future network traffic that uses the same IP address. IP actions are similar to other actions; they direct the device to drop or close the connection. However, because you now also have the attacker’s IP address, you can choose to block the attacker for a specified amount of time. If attackers cannot immediately regain a connection to your network, they might try to attack easier targets.

Use IP actions in conjunction with actions and logging to secure your network. In a rule, first configure an action to detect and prevent current malicious connections from reaching your address objects. Then, right-click in the IP Action column of the rule and select Configure to bring up the Configure IP Action dialog box. Enable and configure an IP action to prevent future malicious connections from the attacker’s IP address.

Choosing an IP Action
For each IP action option, an IP action is generated by the NetScreen-Security Manager system. The IP action instructs the security device to perform the specified task. Select from the following options:

- **IDP Notify**—The security device does not take any action against future traffic, but logs the event. This is the default.
- **IDP Drop**—The security device drops the matching connection and blocks future connections that match the criteria set in the Block list.
- **IDP Close**—The security device closes future connections that match the criteria in the Block list.

Choosing a Block Option
Each block option follows the criteria you set in the Actions box. Block options can be based on the following matches of the attack traffic:

- **Source, Destination, Destination Port and Protocol**—The security device blocks future traffic based on the source, destination, destination port, and protocol of the attack traffic. This is the default.
- Source—The security device blocks future traffic based on the source of the attack traffic.

- Destination—The security device blocks future traffic based on the destination of the attack traffic.

- From Zone, Destination, Destination Port and Protocol—The security device blocks future traffic based on the source zone, destination, destination port, and protocol of the attack traffic.

- From Zone—The security device blocks future traffic based on the source zone of the attack traffic.

**Setting Logging Options**

When the security device detects attack traffic that matches a rule and an IP action is triggered, the device can log information about the IP action that was taken or create an alert in the Log Viewer. By default, there are no logging options set.

**Setting Timeout Options**

You can set the number of seconds that you want the IP action to remain in effect after a traffic match. For permanent IP actions, leave the timeout at 0 (this is the default).

**Configuring Notification in IDP Rules**

You can choose to log an attack and create log records with attack information that you can view real-time in the Log Viewer. For more critical attacks, you can also set an alert flag to appear in the log record.

To log an attack for a rule, right-click the Notification column of the rule and select Configure. The Configure Notification dialog box appears.

The first time you design a Security Policy, you might be tempted to log all attacks and let the policy run indefinitely. Don’t do this! Some attack objects are informational only, and others can generate false positives and redundant logs. If you become overloaded with data, you can miss something important. Remember that Security Policies that generate too many log records are hazardous to the security of your network, as you might discover an attack too late or miss a security breach entirely due to sifting through hundreds of log records. Excessive logging can also affect throughput, performance, and available disk space. A good Security Policy generates enough logs to fully document only the important security events on your network.

- Setting Logging—In the Configure Notification dialog box, select Logging and then click OK. Each time the rule is matched, the NetScreen-Security Manager system creates a log record that appears in the Log Viewer.

- Setting an Alert—In the Configure Notification dialog box, select Alert and then click OK. If Alert is selected and the rule is matched, the security device places an alert flag in the Alert column of the Log Viewer for the matching log record.
Logging Packets—You can record the individual packets in the network traffic that matched a rule by capturing the packet data for the attack. Viewing the packets used in an attack on your network can help you determine the extent of the attempted attack and its purpose, whether or not the attack was successful, and any possible damage to your network.

NOTE: To improve performance, log only the packets after the attack.

If multiple rules with packet capture enabled match the same attack, the security device captures the maximum specified number of packets. For example, you configure Rule 1 to capture 10 packets before and after the attack, and Rule 2 to capture 5 packets before and after the attack. If both rules match the same attack, IDP attempts to capture 10 packets before and after the attack.

NOTE: Packet captures are restricted to 9999 packets before and after the attack.

Setting Severity for IDP Rules

(This column only appears when you view the Security Policy in Expanded Mode. To change the Security Policy view from Compact Mode to Expanded Mode, from the menu bar, select View > Expanded Mode.)

You can override the inherent attack severity on a per-rule basis within the IDP rulebase. You can set the severity to either Default, Info, Warning, Minor, Major, or Critical.

To change the severity for a rule, right-click the Severity column of the rule and select a severity.

Setting Target Security Devices for IDP Rules

For each rule in the IDP rulebase, you can select the security device on which the rule is installed. When you install the Security Policy that the rule belongs to, the rule becomes active only on the device(s) you selected in the Install On column of the rulebase.

NOTE: The NetScreen-Security Manager supports IDP only on an ISG 2000 or ISG 1000 security device running ScreenOS 5.0.0-IDP1.

Entering Comments for IDP Rules

You can enter notations about the rule in the Comments column. Anything you enter in the Comments column is not pushed to the target device(s). To enter a comment, right-click the Comments column and select Edit Comments. The Edit Comments dialog box appears. You can enter up to 1024 characters in the Comments field.
EXAMPLE: Configuring Rules for a Standalone IDP System

You can deploy the ISG 2000 or ISG 1000 security device as a standalone IDP security system protecting critical segments of your private network. For example, you might already have a security device actively screening traffic between the Internet and your private network (some device can optionally use Deep Inspection to inspect this traffic), but you still need to protect internal systems, such as mail servers, from attacks that might originate from user machines in an otherwise trusted network. In this case, you need a security system that provides IDP instead of firewall functions.

Juniper Networks offers "standalone" NetScreen-IDP appliances that provide IDP functionality without integrated FW/VPN capabilities. You cannot use the NetScreen-Security Manager system to manage these appliances. NetScreen-Security Manager supports IDP only on the ISG 2000 and ISG 1000 devices.

In this example, you are deploying a ISG 2000 or ISG 1000 device as a standalone IDP security system between the Trust zone and the custom “Data_Center” zone in your network. Your company’s file, mail, and database servers reside in the Data_Center zone. While you want to allow users in the Trust zone to be able to access the servers in the Data_Center zone, you also need to protect the servers from attacks that inadvertently might have been introduced into a user machine in the Trust zone. You create a firewall rule from the Trust to the Data_Center zone that allows traffic from any source to any destination for any service, then enable IDP in the Rule Options column, as shown in the following:

Figure 130: Firewall Rule for Dedicated IDP

You would then add and configure IDP rulebases for the Security Policy to detect possible attacks against servers in the Data_Center zone.

Figure 131: IDP Rules for Dedicated IDP

Configuring Exempt Rules
Chapter 9: Configuring Security Policies

The Exempt rulebase works in conjunction with the IDP rulebase. Before you can create exempt rules, you must first create rules in the IDP rulebase. If traffic matches a rule in the IDP rulebase, IDP attempts to match the traffic against the Exempt rulebase before performing the specified action or creating a log record for the event.

NOTE: If you delete the IDP rulebase, the Exempt rulebase is also deleted.

You might want to use an exempt rule when an IDP rule uses an attack object group that contains one or more attack objects that produce false positives or irrelevant log records. To prevent unnecessary alarms, you might want to use an exempt rule to exclude a specific source, destination, or source/destination pair from matching an IDP rule.

When you create an exempt rule, you must specify the following:

- Source and destination for traffic you want to exempt. You can set the source or destination to “any” to exempt network traffic originating from any source or sent to any destination. You can also specify “negate” to specify all sources or destinations except the specified addresses.
- The attacks you want IDP to exempt for the specified source/destination addresses. You must include at least one attack object in an exempt rule.

NOTE: The Exempt rulebase is a non-terminal rulebase. That is, IDP attempts to match traffic against all rules in the Exempt rulebase and all matches are executed.

Adding the Exempt Rulebase

Before you can configure a rule in the Exempt rulebase, you need to add the Exempt rulebase to a Security Policy.

1. In the main navigation tree, select Security Policies. Open a security policy by double-clicking the policy name in the Security Policies window or click the policy name and then select the Edit icon.

2. Click the Add icon in the upper right corner of the Security Policy window and select Add Exempt Rulebase. The Exempt rulebase tab appears.

3. To configure an exempt rule, click the Add icon on the left side of the Security Policy window. A default exempt rule appears. You can modify this rule as needed.

Defining Match

You specify the traffic you want to exempt from attack detection. The Match columns From Zone, Source, To Zone, and Destination are required for all rules in the exempt rulebase.

The following sections detail the Match columns of an exempt rule.
Configuring Source & Destination Zones

You can select multiple zones for the source and destination, however these zones must be available on the security devices on which you will install the policy. You can specify “any” for the source or destination zones to monitor network traffic originating or destined for any zone.

NOTE: You can create custom zones for some security devices. The list of zones from which you can select source and destination zones includes the predefined and custom zones that have been configured for all devices managed by NetScreen-Security Manager. Therefore, you should only select zones that are applicable for the device on which you will install the Security Policy.

Configuring Source & Destination Address Objects

In the NetScreen-Security Manager system, address objects are used to represent components on your network: hosts, networks, servers, etc. You can specify “any” to monitor network traffic originating from any IP address. You can also negate the address object(s) listed in the Source or Destination column to specify all sources or destinations except the excluded object.

You can create address objects either before you create an exempt rule or while creating or editing an exempt rule. To select or configure an address object, right-click either the Source or Destination column of a rule and select Select Address. In the Select Source Addresses dialog box, you can either select an already-created address object or click the Add icon to create a new host, network, or group object.

EXAMPLE: EXEMPTING A SOURCE/DESTINATION PAIR

To improve performance and eliminate false positives between your Internal Lab devices and your Engineering desktops, you want to exempt attack detection. Your exempt rule looks similar to the one below:

Figure 132: Exempting Source and Destination

Setting Attack Objects

You specify the attack(s) you want IDP to exempt for the specified source/destination addresses. You must include at least one attack object in an exempt rule.
EXAMPLE: EXEMPTING SPECIFIC ATTACK OBJECTS

You consistently find that your Security Policy generates false positives for the attack HTTP Buffer Overflow: Header on your internal network. You want to exempt attack detection for this attack when the source IP is from your internal network. Your exempt rule looks similar to the one below:

Figure 133: Exempting Attack Object

Setting Targets

For each rule in the Exempt rulebase, you can select the ISG 2000 or ISG 1000 device that will use that rule to detect and prevent attacks. When you install the Security Policy that the rule belongs to, the rule becomes active only on the device(s) you select in the Install On column of the rulebase.

Entering Comments

You can enter notations about the rule in the Comments column. Anything you enter in the Comments column is not pushed to the target device(s). To enter a comment, right-click the Comments column and select Edit Comments. The Edit Comments dialog box appears. You can enter up to 1024 characters in the Comments field.

Creating an Exempt Rule from the Log Viewer

You can also create a rule in the Exempt rulebase directly from the NetScreen-Security Manager Log Viewer. You might want to use this method to quickly eliminate rules that generate false positive log records. (For more information about viewing IDP logs, see “Review IDP Logs” on page 45.) For more information about using the Log Viewer, see “Logging” on page 719.

To create an exempt rule from the Log Viewer:

1. View the IDP/DI logs in the Log Viewer.
2. Right-click a log record that contains an attack you want to exempt and select Exempt.

NOTE: NetScreen-Security Manager supports IDP only on an ISG 2000 or ISG 1000 device.
Configuring Backdoor Rules

A backdoor is a mechanism installed on a host computer that facilitates unauthorized access to the system. Attackers who have already compromised a system can install a backdoor to make future attacks easier. When attackers type commands to control a backdoor, they generate interactive traffic.

Interactive traffic is traffic that indicates human involvement in a normally automated process, such as a user typing commands. Interactive traffic looks different than other traffic because humans are manually controlling one end of the connection. In a connection between two programs, the data transfer is automated; TCP packets can be batched and sent in bulk for efficiency. In a connection between a program and a user, packets are sent when they become available; characters display as they are typed (not after the word is complete). Interactive programs transmit several short IP packets containing individual keystrokes and their echoes, reflecting the real-time actions of a user (or attacker).
When attackers type commands to control a backdoor, they generate interactive traffic that IDP can detect. Unlike anti-virus software, which scans for known backdoor files or executables on the host system, IDP detects the interactive traffic that is produced when backdoors are used. This method ensures that IDP can detect all backdoors, both known and unknown. If interactive traffic is detected, IDP can perform IDP actions against the connection to prevent the attacker from further compromising your network.

When you configure a backdoor rule, you must specify the following:

- Source and destination addresses for traffic you want to monitor. To detect incoming interactive traffic, set the Source to “any” and the Destination to the IP address of network device you want to protect. To detect outgoing interactive traffic, set the Source to the IP address of the network device you want to protect and the Destination to “any”.

- Services that are offered by the Source or Destination as well as interactive services that can be installed and used by attackers.

NOTE: Do not include TELNET, SSH, RSH, NETMEETING, or VNC as services, as these services are often used to legitimately control a remote system. Including these services can generate false positives.

- Action that the IDP is to perform if interactive traffic is detected. Set the Operation to “detect”. If you are protecting a large number of network devices from interactive traffic, you can create a rule that “ignores” accepted forms of interactive traffic from those devices, then create another rule that “detects” all interactive traffic from those devices.

NOTE: The Backdoor rulebase is a terminal rulebase. That is, when IDP finds a match on a rule in the Backdoor rulebase, it does not execute succeeding rules.

Adding the Backdoor Rulebase

Before you can configure a rule in the Backdoor rulebase, you need to add the Backdoor rulebase to a Security Policy.

1. In the main navigation tree, select Security Policies. Open a security policy by double-clicking the policy name in the Security Policies window or click the policy name and then select the Edit icon.

2. Click the Add icon in the upper right corner of the Security Policy window and select Add Backdoor Rulebase. The Backdoor rulebase tab appears.

3. To configure a backdoor rule, click the Add icon on the left side of the Security Policy window. A default backdoor rule appears. You can modify this rule as needed.

Defining Match

You specify the traffic you want to IDP to monitor for indications of backdoors or Trojans. The Match columns From Zone, Source, To Zone, Destination, and Service are required for all rules in the Backdoor rulebase.
The following sections detail the Match columns of a backdoor rule.

Configuring Source & Destination Zones

You can select multiple zones for the source and destination, however these zones must be available on the security devices on which you will install the policy. You can specify “any” for the source or destination zones to monitor network traffic originating or destined for any zone.

NOTE: You can create custom zones for some security devices. The list of zones from which you can select source and destination zones includes the predefined and custom zones that have been configured for all devices managed by NetScreen-Security Manager. Therefore, you should only select zones that are applicable for the device on which you will install the Security Policy.

Configuring Source & Destination Address Objects

In the NetScreen-Security Manager system, address objects are used to represent components on your network: hosts, networks, servers, etc. Typically, a server or other device on your network is the destination IP for incoming attacks, and can sometimes be the source IP for interactive attacks. You can specify “any” to monitor network traffic originating from any IP address. You can also negate the address object(s) listed in the Source or Destination column to specify all sources or destinations except the excluded address object.

You can create address objects either before you create a backdoor rule or while creating or editing a backdoor rule. To select or configure an address object, right-click either the Source or Destination column of a rule and select Select Address. In the Select Source Addresses dialog box, you can either select an already-created address object or click the Add icon to create a new host, network, or group object.

Configuring Services

Select interactive service objects. Be sure to include services that are offered by the source or destination IP as well as interactive services that are not; attackers can use a backdoor to install any interactive service. Do not include telnet, SSH, RSH, netmeeting, or VNC, as these services are often used to remotely control a system legitimately and their inclusion might generate false positives.

Setting Operation

Set the Operation to detect or ignore. If you select detect, choose an action to perform if backdoor traffic is detected. If you are protecting a large number of address objects from interactive traffic, you can create a rule that ignores accepted forms of interactive traffic from those objects, then create a succeeding rule that detects all interactive traffic from those objects.

Setting Actions

Choose an action to perform if IDP detects interactive traffic:
Table 32: Actions for Backdoor Rule:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept</td>
<td>IDP accepts the interactive traffic.</td>
</tr>
<tr>
<td>Drop Connection</td>
<td>IDP drops the interactive connection without sending a RST packet to the sender, preventing the traffic from reaching its destination. Use this action to drop connections for traffic that is not prone to spoofing.</td>
</tr>
<tr>
<td>Close Client and Server</td>
<td>IDP closes the interactive connection and sends a RST packet to both the client and the server. If the IDP is in sniffer mode, IDP sends a RST packet to both the client and server but does NOT close the connection.</td>
</tr>
<tr>
<td>Close Client</td>
<td>IDP closes the interactive connection to the client, but not to the server.</td>
</tr>
<tr>
<td>Close Server</td>
<td>IDP closes the interactive connection to the server, but not to the client.</td>
</tr>
</tbody>
</table>

**Setting Notification**

You can choose to log an attack and create log records with attack information that you can view real-time in the Log Viewer. For more critical attacks, you can also set an alert flag to appear in the log record.

To log an attack for a rule, right-click the Notification column of the rule and select Configure. The Configure Notification dialog box appears.

The first time you design a Security Policy, you might be tempted to log all attacks and let the policy run indefinitely. Don't do this! Some attack objects are informational only, and others can generate false positives and redundant logs. If you become overloaded with data, you can miss something important. Remember that Security Policies that generate too many log records are hazardous to the security of your network, as you might discover an attack too late or miss a security breach entirely due to sifting through hundreds of log records. Excessive logging can also affect IDP throughput, performance, and available disk space. A good Security Policy generates enough logs to fully document only the important security events on your network.

**Setting Logging**

In the Configure Notification dialog box, select Logging and then click OK. Each time the rule is matched, the IDP system creates a log record that appears in the Log Viewer.

You can choose to simply log an attack and create log records with attack information that you can view real-time in the Log Viewer. For more critical attacks, however, you might want to be notified immediately by email, have IDP run a script in response to the attack, or set an alarm flag to appear in the log record. Your goal is to fine-tune the attack notifications in your Security Policy to your individual security needs.

**Setting an Alert**

In the Configure Notification dialog box, select Alert and then click OK. If Alert is selected and the rule is matched, IDP places an alert flag in the alert column of the Log Viewer for the matching log record.
Logging Packets

You can record the individual packets in the network traffic that matched a rule by capturing the packet data for the attack. Viewing the packets used in an attack on your network can help you determine the extent of the attempted attack and its purpose, whether or not the attack was successful, and any possible damage to your network.

NOTE: To improve IDP performance, log only the packets after the attack.

If multiple rules with packet capture enabled match the same attack, IDP captures the maximum specified number of packets. For example, you configure Rule 1 to capture 10 packets before and after the attack, and Rule 2 to capture 5 packets before and after the attack. If both rules match the same attack, IDP attempts to capture 10 packets before and after the attack.

NOTE: Packet captures are restricted to 9999 packets before and after the attack.

Setting Severity

You can override the inherent attack severity on a per-rule basis within the Backdoor rulebase. You can set the severity to either Default, Info, Warning, Minor, Major, or Critical.

To change the severity for a rule, right-click the Severity column of the rule and select a severity.

Setting Targets

For each rule in the Backdoor rulebase, you can select the ISG 2000 or ISG 1000 device that will use that rule to detect and prevent attack. When you install the Security Policy that the rule belongs to, the rule becomes active only on the devices you select in the Install On column of the rulebase.

NOTE: The NetScreen-Security Manager supports IDP only on an ISG 2000 or ISG 1000 device.

Entering Comments

You can enter notations about the rule in the Comments column. Anything you enter in the Comments column is not pushed to the target device(s). To enter a comment, right-click the Comments column and select Edit Comments. The Edit Comments dialog box appears. You can enter up to 1024 characters in the Comments field.

Installing Security Policies

After you have successfully verified your Security Policy, you must:

1. Assign the policy to your managed devices
2. Validate the policy
3. Install the policy on your managed devices

The following sections detail each step.

Assigning a Security Policy to a Device

New devices do not have an existing or default Security Policy. However, when you import a device configuration, NetScreen-Security Manager automatically imports all existing policies for the device. To simplify policy management, you can merge these multiple device policies into a single Security Policy that you install on several devices at one time. For details, see “Merging Policies” on page 586.

After you have created a Security Policy, you must assign that policy to a device. Assigning a policy to a device links the device to that policy, enabling NetScreen-Security Manager to install the policy on that device. To assign an existing policy to a device, use one of the following methods:

- Right-click a device and select Policy > Assign Policy. Select the policy you want to assign to the device.
- Double-click a device to open the device configuration. In the Info tab, under Policy for device, select the policy you want to assign to the device.

You can use a single Security Policy to control multiple security devices. Each rule in a Security Policy contains an Install On column that specifies the devices the rule is applied to. This means that you can assign a Security Policy to a device, but only some of the rules in that policy are actually installed on that device during a device update.

You can also create multiple policies for a single device, but only one Security Policy can be active on the device. When you update a device configuration, NetScreen-Security Manager installs the active policy on the security device. By default, NetScreen-Security Manager considers the active policy as the policy that was most recently edited.

NOTE: If you delete and then re-import a device, you must reassign a policy to the device.

Validating Security Policies

You should validate a Security Policy to identify potential problems before you install it. NetScreen-Security Manager contains a Policy Validation tool to help you locate common problems, such as:

- Rule Duplication—Occurs when one or more rules in the Security Policy are identical.
- Zone Mismatch—Occurs when the source or destination zone you have chosen in a rule is not available on the device you selected in the Install column.
- Rule Shadowing—Occurs when two or more rules detect the same traffic. For details, see “Rule Shadowing” on page 578.
Unsupported Options—Occurs when a device in the Install column of a rule does not support a specific rule option configured for the rule. For details, see “Unsupported Options” on page 579.

To use the Policy Validation tool to validate a Security Policy, you must first assign the Security Policy to a device. Then, to validate a policy, from the menu bar click Devices > Policy > Validate Policy. A Job Manager window appears to display job information and progress. Policy validation analyzes the source and destination addresses, the to and from zones, and the service when validating. If NetScreen-Security Manager identifies any problems in the policy during policy validation, it displays information about the problem at the bottom of the selected rulebase.

NOTE: We highly recommend that you validate a policy before installing. A Security Policy that has internal problems can leave your network vulnerable.

Rule Shadowing
Policy validation can identify rule shadowing, a problem that occurs when two rules are designed to detect the same attack. Eliminating rule shadowing in your policy improves the performance of your security device. To correct, return to the rule that is shadowing and modify or delete it. NetScreen-Security Manager validates rules according to the ScreenOS version that is running on the device in the Install On column:

- For ScreenOS 4.0.x devices, each item the rule is treated as a separate rule. For example, a rule with two service objects (AOL and DNS) is sent to the device as two rules, one rule with AOL and another with DNS.

- For ScreenOS 5.x devices, a rule can contain multiple items. For example, a rule with two or more service objects is sent to the device as one rule.

For example, the following policy contains rule shadowing:

Figure 135: View Rule Shadowing Example

<table>
<thead>
<tr>
<th>From Zone</th>
<th>Source</th>
<th>To Zone</th>
<th>Destination</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>untrust</td>
<td>any</td>
<td>dmz</td>
<td>Web Server</td>
<td>DNS</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>HTTP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>PING</td>
</tr>
</tbody>
</table>

If you install this policy on a ScreenOS 4.x device, rule validation fails because rule 2 shadows rule 1 (the device receives two rules from the same source/destination that use HTTP). However, a ScreenOS 5.x device passes.
Unsupported Options

Policy Validation can also identify unsupported options in your Security Policy. Because different security devices and systems support different features and options, policy validation checks the rules in the policy to ensure that the devices specified in the Install On column of the rule can support the Rule Options configured for the rule.

Some examples of unsupported option messages are included below:

- 'Permit/Tunnel' Rules from home zone to work zone is not allowed on a Dial 2 Device (except when NSRP Lite enabled).
- Destination NAT Option not available on 4.0.x devices.
- AntiVirus Option not available on 4.0.x devices.
- Deep Inspection Option not available on 4.0.x devices.
- Reject Action Option not available on 4.0.x and 5.0.x devices.

---

NOTE: Because the “reject” firewall action is supported only by devices running ScreenOS 5.1 and higher, when NetScreen-Security Manager installs this rule on a device running 4.0.x or 5.0.x, the action is automatically changed to “deny”.

- Schedule Option is not supported on a Vsys Device.

For example, if you configure a firewall rule option (such as AntiVirus protection or Deep Inspection) that is not supported by the security device in the Install column of the rule, policy validation displays an information message that describes the unsupported feature.

Figure 136: View Unsupported Feature Warning Message

2 Warning(s) found.
#5: Deep Inspection Option not available on 4.0 devices. Will be trimmed before an Update Device.
#5/Attack Prevention/Attack: When Action is 'deny', Deep Inspection Options are ignored by device.

Installing New Security Policies

Before you install a new Security Policy, ensure that you have:

- Assigned the policy to your devices—After you have created a Security Policy, you must assign that policy to the devices you want to use that policy. Assigning a policy to a device links the device to that policy, enabling NetScreen-Security Manager to install the policy on that device.

- Selected the correct devices for the Install On column of each rule—A security device can only use one Security Policy at a time; when you install a new policy, it overwrites all existing policies on the security device.
- Configured each device in the Install On column of each rule correctly—When you push a policy to a device, you also push the device configuration to the device. Any changes made (by you or another admin) to the device configuration are pushed to the device along with the policy.

- Configured rules in each rulebase correctly—The management system installs rules from all rulebases on the specified device. For details on the rule installation and rule execution sequence, see “Rule Execution Sequence” on page 529.

- Configured the VPN rules or VPN links in the policy correctly—The management system installs all VPN rules in the policy.

Additionally, to help you identify possible problems in your policy, you might want to run a Delta Config Summary before pushing the policy.

During policy installation, NetScreen-Security Manager installs the rules in the policy on the security devices you selected in the Install On column of each rule. The install process occurs between the management system and your managed devices. First, the GUI Server creates the ADM file that contains all policies for all devices selected for update (although the ADM file collects information from all policies, it does not merge the policies) The GUI Server sends the ADM to the Device Server. Next, the NetScreen-Security Manager Device Server receives the ADM and uses it to create a separate, individual DM for each device that you selected for update:

- For 5.x devices, the Device Server sends the DM to the managed device, which translates the information in the DM into commands and runs those commands on the devices.

- For 4.0.x devices and earlier, the Device Server translates the DM into commands and send those commands to the managed device, which runs those commands.

**Figure 137: Install New Security Policies**

For details on the device ADM and DM, see the “Managing Device Capabilities” on page 431.
**Updating Existing Security Policies**

To install a new or modified policy on a managed device, from the toolbar, select Devices > Configuration > Update Device Config. If you changed the device configuration or assigned policy for a device, that device is automatically selected. Unselect any devices you do not want to update.

You can also enable session rematch for policy installations on managed devices running ScreenOS 5.1 or higher. Session rematch enables NetScreen-Security Manager to preserve the existing sessions that are being tracked by the installed Security Policy during the policy update procedure. At the end of the update, NetScreen-Security Manager restores all valid sessions on the managed device and deletes all invalid sessions (a session is considered valid when the From Zone, Source, To Zone, Destination, and Service of the traffic is the same before and after the new policy installation).

You enable session rematch when you update devices (from the menu bar, select Devices > Configuration > Update Device Config). To enable session rematch from the Update Devices dialog box, select Options, then select Rematch, session treatment when modifying a policy rule, then click OK.

---

**NOTE:** You can also enable/disable session rematch in the system-wide device update settings. To configure, from the menu bar, select Tools > Preferences > Device Update. The system-wide setting (enabled or disabled) becomes the default setting for all device updates, but you can change the setting as needed for each individual update.

After you have selected the devices you want to update (and configured session rematch, if desired), click OK to begin the update process. The Job Manager dialog box appears and displays the progress of the policy installation. As the update is performed, the main display area of the Job Manager dialog box displays the CLI commands that the management system is sending to the physical device. In some cases, you might see that the policy is unset, then reset on the device.

NetScreen-Security Manager does not need to reset the policy when:

- The Security Policy you are installing does not exists on the physical device. The update installs the Security Policy on the device.

- The Security Policy you are installing already exists on the physical device. The update simply modifies the policy on the physical device, without resetting the policy.

NetScreen-Security Manager **must reset the policy** when the Security Policy you are installing already exists on the physical device, but an object within the policy has changed in NetScreen-Security Manager. The update first unsets the current policy on the device, deletes the old object, adds the new changed object, then installs the entire Security Policy again on the physical device.

---

**NOTE:** Additionally, NetScreen-Security Manager must reset the policy during an import when the Security Policy exists on the device, but does not exist in the management system.
After the updated has completed, close the Job Manager window. The rules in the policy become active on the devices you selected in the Install On column of the rule. To see the exact rules that were applied to a specific device, in Device Manager, right-click a device and select Policy > View Pending Device Policy.

Managing Rules and Policies

Managing rules and policies for multiple security devices can seem daunting at first. Take some time to carefully design your policies to make them efficient.

- Helpful Tips
- Using Zone Exceptions
- Using Zone Filters
- Selecting Rules
- Editing Rule Order
- Using Cut, Copy, and Paste
- Deleting a Rule
- Disabling a Rule
- Using Rule Groups
- Re-Importing Devices & Security Policies
- Merging Policies
- Exporting Policies

Helpful Tips

Some helpful tips about managing your rules and policies:

- Because a device can have only one Security Policy installed at a time, you must include all rules for that device in one policy.


- Each Security Policy contains a default firewall rulebase (Zone); you can add other rulebases (Global, Multicast, IDP, Exempt, Backdoor) to create additional rules.

- Each rulebase can contain one or more rules, up to 40,000 max for the Security Policy. The top rule in the rulebase is rule 1, and second rule is rule 2, and so on. To combine rules for easier management within the Zone rulebase, you can create rule groups.
Each rule group can contain one or more rules, up to 40,000 max for the Security Policy. Rules within a rule group follow the rulebase numbering sequence.

The IDP, Exempt, or Backdoor rulebases are not included when you:

- Merge two policies into a single policy
- Import a Security Policy from an existing IDP-capable security device

You cannot disable an entire Security Policy or a rulebase. You can, however, disable individual rules; for details, see “Disabling a Rule” on page 585.

When you re-import a device that was previously managed by NetScreen-Security Manager, you must manually re-assign a policy to a re-imported device. For details on re-importing issues, see “Re-Importing Devices & Security Policies” on page 586.

Using Zone Exceptions

A zone exception is a powerful tool that can help reduce the number of rules in your Security Policy while maintaining the same functionality. Zone exceptions add flexibility to your rules, enabling you to include more devices in a single rule. You can add multiple zone exceptions for the To Zone or From Zone of a rule in the Zone rulebase.

To configure a zone exception, in the To Zone or From Zone column of a rule, right-click and select Select Zone Exception. Configure a zone and the device on which that zone is configured. When you update your managed devices with the Security Policy and the rule is installed on the security device, the zone exception for that device appears as the designated To Zone or From zone.

EXAMPLE: USING ZONE EXCEPTIONS

In this example, you want to configure a rule in your Security Policy that controls all traffic from the trust zone to the untrust zone on two security devices. However, one device, the NS-208A, contains a DMZ zone through which all traffic from trust and untrust zones must pass. Using a zone exception, you enable the NS-208A to use the DMZ zone instead of the trust zone as the From Zone value.

To configure this zone exception in a rule:

1. In the main navigation tree, select Security Policies. In the main display area, click the Add icon to display the New Security Policy dialog box. Enter a name for the policy, click OK, then select the policy in the main navigation tree.

2. Modify the default rule:

   - In the Action column, right-click and select Permit.
   - In the Install On column, right-click and select the Corsica and NS-208A security devices.

3. Configure the zone exception:
a. In the From Zone column of the rule, right-click and select Select Zone Exceptions. The Zone Exceptions dialog box appears.

b. Click the Add icon to display the New Zone Exceptions dialog box. Configure as shown below, then click OK:

Figure 138: Zone Exceptions Example

- For Zone, select dmz.
- For Device, select the NS-208A security device.

c. Click OK again to save the zone exception to the rule, which now appears as shown below:

Figure 139: Zone Exceptions Example Rule

<table>
<thead>
<tr>
<th>Zone Exceptions</th>
<th>New Zone Exception</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zone</td>
<td>Device</td>
</tr>
<tr>
<td>dmz</td>
<td>NS-208A</td>
</tr>
</tbody>
</table>

Using Zone Filters

To view rules that handle traffic between zones, use the Filter on From and To Zones menus in the Zone rulebase.

Selecting Rules

To select a single rule, click anywhere in the rule; to select multiple rules, press CTRL and select the desired rules.

Editing Rule Order

To change the order of rules in a policy, right the No. Column (the first column) of a rule and select Move Rule Up or Move Rule Down.
Using Cut, Copy, and Paste

To quickly create multiple rules that use the same basic information, copy and paste the rule, then change the parameters in each copied rule to make the rule unique (this is especially useful for rules that contain detailed rule options such as attack protection).

To cut and paste a rule, right-click inside the No. column (the first column) of the rule and select Edit > Cut. Next, select a rule that is above or below the position you want to paste the cut rule into, then select Edit > Paste > <above> <below>.

NOTE: The cut rule remains visible in its original position until you paste it into its new position.

Deleting a Rule

To delete a rule, right-click inside the No. column (the first column) of the rule and select Delete. You can also delete a rule group; however, deleting the rule group also deletes all rules within the rule group.

Disabling a Rule

To disable a rule, right-click inside the No. column (the first column) of the rule and select Disable. The rule remains in the rulebase, but displays a gray diagonal stripe to indicate that it has been disabled. While the rule is disabled, NetScreen-Security Manager does not install the rule on any devices.

To enable a rule, right-click inside the No. column (the first column) of the rule and select Disable again to clear the checkbox. You can disable rule groups using the same method.

Using Rule Groups

To create a rule group, press Ctrl and select the rules you want to include in the group, then right-click and select create rule group. Enter a name and description for the rule group, then click OK.

Combining rules into a rule group can help you better manage rules. For example, you might want to create rule group for:

- VPN rules or VPN links
- Rules that manage traffic from a specific zone or interface on the security device
- Rules for a specific device or device group
- Rules that provide attack or AV protection
- Rules that manage VoIP traffic with GTP objects

You can add, edit, and delete rule groups; however, deleting a rule group also deletes all rules within that group. If necessary, you can also ungroup a rule group.
You can create multiple rule groups (40,000 rules max in a Security Policy). NetScreen-Security Manager supports one level of rule groups; you cannot create a rule group within a rule group.

Re-Importing Devices & Security Policies

Occasionally, you might need to delete and then re-add a security device to NetScreen-Security Manager. After you re-import the device configuration for a device that was previously managed by NetScreen-Security Manager:

- If you made no changes to the device policies using the WebUI or CLI, when you re-import the device, NetScreen-Security Manager does not create a new Security Policy.
- If you made changes to the device policies using the WebUI or CLI, when you re-import the device, NetScreen-Security Manager creates a new Security Policy.

You must manually re-assign a policy to a re-imported device. For example, if you re-import a previously-managed security device, you might want to first merge the imported policy with a more comprehensive policy, then assign the comprehensive policy to the device.

**NOTE:** Importing the running configuration from a device completely overwrites all configuration information stored within NetScreen-Security Manager for that device. To help avoid accidental configuration overwriting, when you attempt to import a configuration from a currently managed security device, NetScreen-Security Manager prompts you for confirmation to import.

Merging Policies

When you import policies from a single managed device, those policies appear in NetScreen-Security Manager as rules in a new policy. Each device policy is imported as a single rule, and the rules make up the policy that exists on the device.

**NOTE:** In the ScreenOS WebUI and CLI, a Security Policy is a single statement that defines a source, destination, zone, direction, and service. In NetScreen-Security Manager, those same statements are known as rules, and a Security Policy is a collection of rules.

To simplify policy management and maintenance, you can merge two policies into a single Security Policy. To merge two policies, select a source policy and a target policy:

- The source policy contains the rules that you want to merge into another policy (in the UI, this is the From Policy).
- The target policy receives the rules from the source policy (in the UI, this is the To Policy).
NetScreen-Security Manager copies the rules from the source policy and pastes them above, below, or inline with the rules in the target policy. When placing rules inline, be aware of the intra-policy dependence of both policies. Because rule order is important (rules are executed top-down), rules can be dependant on other rules. If you rearrange the order of dependant rules by inserting merged rules, the security device changes the way it handles the packets. If you are unsure if you have intra-policy dependence in your rules, it’s best to merge rules above or below the existing rules.

After creating a single Security Policy that contains both source and target rules, NetScreen-Security Manager also identifies rules that contain similar values in the source, destination, service, and install on columns, then collapses those rules into a single rule. NetScreen-Security Manager does not collapse rules that contain different zones, or rules that refer to unique VPNs.

By default, NetScreen-Security Manager also updates the device policy pointers to reference the new merged policy (the device policy pointer indicates which Security Policy is assigned to a device). When configuring Policy Merge settings, you can edit this option to keep the device policy pointers for both the source and target policies.

You can merge any two Security Policies. To access the Policy Merge tool, select the Security Policies, then use the menu bar to select Tools > Policy Merge. See the NetScreen-Security Manager Online Help for details.

**NOTE:** You can merge rules from 4.0.x or 5.0.x devices that use the deny action into rules from 5.1 or higher devices that use the reject action, provided that the source, destination, source, and service are the same for the rules. NetScreen-Security Manager automatically subsumes the deny action into the reject action for rules imported or merged from 4.0.x and 5.0.x devices; when the merged Security Policy is installed on the device however, the action appears as deny for 4.0.x and 5.0.x devices and as reject for 5.1 and higher devices.

**EXAMPLE: MERGING SECURITY POLICIES**

Policy A contains the following rules:

*Figure 140: Security Policy A Rules (Before Policy Merge)*

<table>
<thead>
<tr>
<th>No.</th>
<th>From Zone</th>
<th>Source</th>
<th>To Zone</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>trust</td>
<td>1.1.1.1</td>
<td>untrust</td>
<td>2.2.2.2</td>
<td>FTP</td>
<td>permit</td>
<td>Boston</td>
</tr>
<tr>
<td>2</td>
<td>trust</td>
<td>3.3.3.3</td>
<td>untrust</td>
<td>4.4.4.4</td>
<td>HTTP</td>
<td>permit</td>
<td>Paris</td>
</tr>
<tr>
<td>3</td>
<td>trust</td>
<td>5.5.5.5</td>
<td>untrust</td>
<td>6.6.6.6</td>
<td>ICMP-ANY</td>
<td>permit</td>
<td>Bczeman</td>
</tr>
</tbody>
</table>

Policy B contains the following rules:
To merge Policy A (from policy) with Policy B (to policy), from the file menu, select Tools > Policy Merge Tool and configure the merge as shown below:

NetScreen-Security Manager copies all rules from Policy A and pastes them above the rules in Policy B. Next, NetScreen-Security Manager merges the matching values in the columns to create a single, simplified policy (Policy C):
Exporting Policies

You can export a security policy rulebase to an HTML file.

To export a security policy, select File > Export Policy. (You can also use the button or Alt-E.) In the Export Policy dialog box, select the rulebases you wish to export. Indicate whether you want to display expanded rule groups and whether you want to see the expanded view. Click the Browse button to select a default export directory for all future exports. Click Export to export the file.

Each export creates a new directory. The default directory name is <policyname>_YYMMDD_HHMMSS. The export process puts each rulebase in a separate HTML file in that directory.

Use an HTML browser to view the exported file. Expanded views may make the output too wide for a standard printer.

EXAMPLE: EXPORTING ZONE BASED FIREWALL RULES WITH EXPANDED VIEW
To export an expanded view of the Zone based Firewall Rules from a security policy, select a policy from Security Policies. Then select File > Export Policy from the menu bar. In the dialog box, select Zone based Firewall Rules. Select Show Expanded View. Browse to an export directory and click Select Export Directory. Click Export.
Figure 144: Export Policy Dialog with Options Selected

NetScreen-Security Manager creates a new subdirectory for each export. To view the policy, point your browser at the file zone.html in the created subdirectory.
Chapter 10
Configuring VPNs

VPNs route private data through a public Internet. Like normal Internet traffic, data in a VPN is routed from source to destination using public Internet networking equipment. Unlike normal traffic, however, the source and destination use a Security Association (SA) pair to create a secure, private tunnel through which the data traverses the Internet. A tunnel has a defined start point and end point, (usually an IP address), and is a private connection through which the data can move freely. By encrypting and authenticating the data while in the tunnel, you can ensure the security and integrity of the data.

VPNs can also connect widely distributed networks to make separate networks appear as a single Wide Area Network (WAN). VPNs replace costly point-to-point protocol (PPP) and frame relay connections that require dedicated lines (and sometimes even satellites!) between your private networks.

The following sections are in this chapter:

- About VPNs
- Planning for Your VPN
- Preparing VPN Components
- Creating VPNs with VPN Manager
- VPN Manager Examples
- Creating Device-Level VPNs
- Device-Level VPN Examples

This chapter discusses the concepts involved in creating secure tunnels between devices, details the differences between VPN types, helps you determine the best VPN for your network, and guides you through creating and configuring your chosen VPN.

NOTE: For step-by-step instructions on creating VPNs, see the NetScreen-Security Manager Online Help Topic “VPNs"
About VPNs

With Juniper Networks NetScreen-Security Manager, you can use basic networking principles and your Juniper Networks security devices to create VPNs that connect your headquarters with your branch offices and your remote users with your protected networks.

NetScreen-Security Manager supports tunnel and transport modes for AutoKey IKE, Manual Key, L2TP, and L2TP-over-AutoKey IKE VPNS in policy or route-based configurations. You can create the VPN at the system-level or device-level:

- **System-Level VPN (VPN Manager)**—Design a system level VPN and automatically set up connections, tunnels, and rules for all devices in the VPN.

- **Device-Level VPN (Device Manager)**—Manually configure VPN information for each security device, then add VPN rules to a Security Policy to create a policy-based VPN or configure routes on each security device to create a route-based VPN.

---

**NOTE:** Each VPN that a device belongs to reduces the maximum number of templates by one. This includes VPNs configured in VPN Manager and VPNs configured at the device-level. You can apply a maximum of 63 templates to a single device.

---

Creating System-Level VPNs with VPN Manager

For AutoKey IKE and L2TP VPNS, create the VPN at the system-level using VPN Manager. VPN Manager supports:

- **AutoKey IKE VPNs**—In policy-based or route-based modes. You can also create a Mixed-Mode VPN to connect policy-based VPN members to route-based VPN members in a single VPN.

- **L2TP-over-AutoKey IKE RAS VPNs and L2TP RAS VPNs**—Can connect and authenticate multiple L2TP remote access services (RAS) users and protected resources with or without encryption.

- **Re-usable VPN Components**—Create objects to represent your protected resources, CA certificates and CRLs, custom IKE proposals, and NAT configurations, then use these objects in multiple VPNs.

- **Compact and Expanded Views**—Choose the Compact (default) or Expanded view to create your VPN. Both views offer the same configuration options.

- **Autogenerated Tunnels**—Create tunnel interfaces on each route-based VPN member automatically. Use the device tunnel summary to review all autogenerated tunnels in the VPN.

- **Autogenerated VPN Rules**—Create all VPN rules with a single click. NetScreen-Security Manager automatically generates the rules between each policy-based VPN member. You can review these rules, configure additional rule options (such as traffic shaping, attack protection, and logging), then insert the rules into a Security Policy.
Planning for Your VPN

To view all VPNs created with VPN Manager, select VPN Manager in the navigation tree. A list of saved VPNs appears in the main display area in table format. You can add and delete VPNs from this view.

VPN Manager does not support Manual Key VPNs; to create a Manual Key VPN in NetScreen-Security Manager, you must create the VPN at the device-level in Device Manager.

Creating Device-Level VPNs in Device Manager

For Manual Key VPNs, create the VPN at the device-level by manually configuring VPN information for each security device.

After you have configured the VPN on each security device in the VPN, add VPN rules to a Security Policy to create the VPN tunnel (for policy-based VPNs) or to control traffic through the tunnel (for route-based VPNs).

You can also create AutoKey IKE, L2TP, and L2TP-over-AutoKey IKE VPNs at the device-level.

Supported VPN Configurations

NetScreen-Security Manager supports all possible VPN configurations that are supported by the CLI and Juniper Networks ScreenOS WebUI, including:

- **NAT-Traversal**—Because NAT obscures the IP address in some IPSec packet headers, VPN nodes cannot receive VPN traffic that passes through an external NAT device. To enable VPN traffic to traverse a NAT device, you can use NAT Traversal (NAT-T) to encapsulate the VPN packets in UDP. If a VPN node with NAT-T enabled detects an external NAT device, it checks every VPN packet to determine if NAT-T is necessary.

- **XAuth**—To authenticate remote access services (RAS) users, use XAuth to assign users an authentication token (such as SecureID) and to make TCP/IP settings (IP address, DNS server, and WINS server) for the peer gateway.

Planning for Your VPN

NetScreen-Security Manager offers you maximum flexibility for creating a VPN. You can choose your topology, authentication level, and creation method. Because you have so many choices, it’s a good idea to determine what your needs are before you create the VPN so you can make the right decisions for your network.

These decisions include:

- **VPN Topology**—What do you want to connect? How many devices? How do you want these devices to communicate? Will you have users as VPN members?

- **Data Protection**—How much security do you need? Do you need encryption, authentication, or both? Is security more or less important than performance?

- **Tunnel Type**—Do you want an always-on connection or traffic-based connection?
Planning for Your VPN

VPN Manager or Device-Level—How do you want to create the VPN? Maintain the VPN?

The following sections provide information to help you make these decisions.

Determining Your VPN Members and Topology

You can use a VPN to connect:

- Security devices—Create a VPN between two or more security devices to establish secure communication between separate networks.
- Network components—Create a VPN between two or more network components to establish secure communication between specific machines.
- Remote users—Create a VPN between a user and a security device to enable secure access to protected networks.

NOTE: In NetScreen-Security Manager, remote users are known as remote access service (RAS) users.

Each device, component, and RAS user in a VPN is considered a VPN node. The VPN connects each node to other nodes using a VPN tunnel. VPN tunnel termination points are the end points of the tunnel; traffic enters and departs the VPN tunnel through these end points. Each tunnel has two termination points: a source and destination, which are the source and destination zones on security device.

Using Network Address Translation (NAT)

Network Address Translation (NAT) maps private IP addresses to public, Internet-routeable IP addresses. Because your security device is also a NAT server, you can use private, unregistered IP addresses for your internal network, minimizing the number of registered IP addresses you must buy and use.

If you enable NAT, when an internal system connects to the Internet, the security device translates the unregistered IP address in the outbound data packets to the registered address of the security device. The security device also relays responses back to the original system. Additionally, because your internal systems do not have a valid Internet IP address, your systems are invisible to the outside Internet, meaning that attackers cannot discover the IP addresses in use on your network.

Site-to-Site

Site-to-site VPNs are the most common type of VPN. Typically, each remote site is an individual security device or RAS user that connects to a central security device.

- Advantages—Simple, easy to configure.
- Disadvantages—The central security device is a single point of failure.

Use a site-to-site VPN to connect remote networks to a single, central network inexpensively. An example is shown below:
Hub and Spoke

In a hub and spoke VPN, multiple security devices (spokes) communicate through a central device (the hub).

- Advantages—Can connect several devices and users. Hub and spoke VPNs are easy to maintain because you only need to reconfigure the spoke and the hub device, which save you administration and resource costs. If you have smaller security devices with limited tunnel capacity, you can use hub and spoke VPNs to increase the number of available tunnels.

- Disadvantages—The hub is a single point of failure; however, you can use NSRP for redundancy.

A hub acts as a concentrator for the other VPN members, but does not necessarily have resources that are available to other members. In fact, you can specify a security device that is not a VPN member to act as the hub: If you include the hub in the VPN, the hub device can send and receive traffic from all spokes; if you do not include the hub, the hub device simply routes traffic between spokes.

Use a hub and spoke topology when you want to route VPN traffic through a VPN member that does not contain protected resources. An example is shown below:
Full Mesh
In a full mesh VPN, all VPN member can communicate with all other VPN members.

- **Advantages**—Because a full mesh configuration uses redundant IPSec tunnels, traffic continues to flow even if a node fails.

- **Disadvantages**—When you add a member to the VPN, you must reconfigure all devices.

Use a full mesh VPN when you need to ensure that every VPN member can communicate with every other VPN member. An example is shown below:
Creating Redundancy

To ensure stable, continuous VPN connection, use redundant gateways to create multiple tunnels between resources. If a tunnel fails, the management system automatically reroutes traffic. Redundant gateways use NSRP to determine the tunnel status.

When planning your VPN topology, consider the importance each tunnel has in the overall network. Critical data tunnels should be redundant to ensure that VPN traffic remains uninterrupted.

Protecting Data in the VPN

To protect traffic as it passes over the Internet, you can create a secure tunnel between devices using a tunneling protocol. Each device in the VPN uses the tunneling protocol to establish a secure data path, enabling traffic between the devices to flow securely from source to destination. NetScreen-Security Manager provides two tunneling protocols, IPSec and L2TP, as detailed in the following sections.

Using IPSec

IPSec is a suite of related protocols that tunnel data between devices and cryptographically secure communications at the network layer. Each device in the VPN has the same IPSec configuration, enabling traffic between the devices to flow securely from source to destination.

Because IPSec functions at the network layer, it protects all data generated by any application or protocol that uses IP. Network layer encryption protects data generated by all protocols at the upper layers of the protocol stack. It also protects all data throughout the entire journey of the packet. Data is encrypted at the source and remains encrypted until reaching its destination. Intermediate systems that transmit the packet (like routers and switches on the Internet) do not need to decrypt the packet to route it, and do not need to support IPSec.
When you create your VPN in NetScreen-Security Manager, you can use one or more IPSec services to establish the tunnel and protect your data. Typically, VPNs use encryption and authentication services to enable basic security between devices; however, for critical data paths, using certificates can greatly enhance the security of the VPN. NetScreen-Security Manager supports the following IPSec data protection services for VPNs.

**Using Authentication**

To authenticate the data in the VPN tunnel, you can use the AH protocol, pre-shared secrets, or certificates:

- **Authentication Header (AH)**—AH authenticates the integrity and authenticity of data in the VPN. You can authenticate packets using Message Digest version 5 (MD5), Secure Hash Algorithm-1 (SHA-1), or Hash-based Message Authentication Code (HMAC).

- **Preshared Secret**—NetScreen-Security Manager generates an ephemeral secret, distributes the secret to each VPN node, then authenticates the VPN data using MD5 or SHA hash algorithms against the secret.

- **Certificates**—IKE uses a trusted authority on the client as the certificate server. For details on using certificates, see “Configuring Certificates” on page 366.

Authentication only authenticates the data; it does not encrypt the data in the VPN. To ensure privacy, you must encrypt the data using ESP.

**Using Encapsulating Security Payload (ESP)**

ESP encrypts the data in the VPN with DES, Triple DES, or AES symmetric encryption. When the encrypted data arrives at the destination, the receiving device uses a key to decrypt the data. For additional security, you can encrypt the keys that decrypt the data using Diffie-Hellman asymmetric encryption. ESP can also authenticate data in the VPN using MD5 and SHA-1 algorithms. You can use ESP to encrypt, authenticate, or encrypt and authenticate data depending on your security requirements.

---

**NOTE:** We strongly recommend that you do not use null AH with ESP.

Because ESP uses keys to encrypt and decrypt data, each VPN node must have the correct key to send and receive VPN data through the VPN tunnel.

You can manually configure a key for each VPN node, or use a key exchange protocol to automate key generation and distribution:

- **Manual Key IKE**—In a manual key VPN, you specify the encryption algorithm, authentication algorithm, and the Security Parameter Index (SPI) for each VPN node. Because all security parameters are static and consistent, VPN nodes can send and receive data automatically, without negotiation.
Autokey IKE—In an AutoKey IKE VPN, you can use the Internet Key Exchange (IKE) protocol to generate and distribute encryption keys and authentication algorithms to all VPN nodes. IKE automatically generates new encryption keys for the traffic on the network, and automatically replaces those keys when they expire. Because IKE generates keys automatically, you can give each key a short life span, making it expire before it can be broken. By also exchanging authentication algorithms, IKE can confirm that the communication in the VPN tunnel is secure.

Because all security parameters are dynamically assigned, VPN nodes must negotiate the exact set of security parameters that will be used to send and receive data to other VPN nodes. To enable negotiations, each VPN node contains a list of proposals; each proposal is a set of encryption keys and authentication algorithms. When a VPN node attempts to send data through the VPN tunnel, IKE compares the proposals from each VPN node and selects a proposal that is common to both nodes. If IKE cannot find a proposal that exists on both nodes, the connection is not established.

IKE negotiations include two phases:

- In Phase 1, two members establish a secure and authenticated communication channel.
- In Phase 2, two members negotiate Security Associations for services (such as IPsec) that require key material and/or parameters.

VPN nodes must use the same authentication and encryption algorithms to establish communication.

Replay protection—In a replay attack, an attacker intercepts a series of legitimate packets and uses them to create a denial-of-service (DoS) against the packet destination or to gain entry to trusted networks. Replay protection enables your security devices to inspect every IPSec packet to see if the packet has been received before—if packets arrive outside a specified sequence range, the security device rejects them.

Using L2TP

Layer 2 Tunneling Protocol (L2TP) is another tunneling protocol used to transmit data securely across the Internet. Because L2TP can transport Point to Point Protocol (PPP) frames over IP, it is often used to:

- Establish PPP connections (Ex. authenticate ADSL services using PPP for users with an ISP at the opposite side of a Telco IP/ATM network)
- Transmit non-IP protocols (Ex. bridge Novell and other network protocols)

PPP can send IP datagrams over a serial link, and is often used to enable dial-up users to connect to their ISP and to the Internet. PPP authenticates username and password, and assigns parameters such as IP address, IP gateway, and DNS. PPP can also tunnel non-IP traffic across a serial link, such as Novell IPX or Appletalk.
PPP is also useful because it can carry non-IP traffic and authenticate connections to RADIUS servers. However, because PPP is not an IP protocol, Internet routers and switches cannot route PPP packets. To route PPP packets, you use L2TP, which encapsulates PPP packet inside an Internet routeable, UDP packet. L2TP VPNs support remote access service users using Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP) authentication.

Using L2TP Over AutoKey IKE

L2TP only transmits packets; for encryption, authentication, or other data protection services, you must further encapsulate the L2TP packet using AutoKey IKE.

Choosing a VPN Tunnel Type

You can configure three types of VPN tunnels with NetScreen-Security Manager:

- Policy-based VPNs—The VPN tunnel is created and maintained only during the transfer of network traffic that matches a VPN rule, and is torn down when the connection ends. Use policy-based VPNs when you want to encrypt and authenticate certain types of traffic between two VPN members.

- Routing-based VPNs—The VPN tunnel is created when the route is defined and is maintained continuously. Use route-based VPNs when you want to encrypt and authenticate all traffic between two VPN members. You cannot add RAS users in a routing-mode VPN.

- Mixed-mode VPNs—Connects policy-based VPNs to route-based VPNs in a mixed-mode VPN. You cannot add RAS users in a mixed-mode VPN.

The following sections detail each VPN type.

About Policy-Based VPNs

A policy-based VPN tunnels traffic between two security devices, or between one security device and a remote user. Each time a security device detects traffic that matches the from zone, source, to zone, destination, and service in the VPN rule, NetScreen-Security Manager creates a VPN tunnel to encrypt, authenticate, and send the data to the specified destination. When no traffic matches the VPN rule, NetScreen-Security Manager tears down the VPN tunnel.

To create a policy-based VPN, you determine the network components you want to protect, and create protected resources to represent those components in the NetScreen-Security Manager UI. A protected resource is a combination of a network component and a service; protected resources in a VPN can communicate with other protected resources using the specified services. In a VPN rule, you add protected resources as the source and destination IP addresses.

Policy-based VPNs can use any of the supported data protection methods. Use policy-based VPNs when you want to enable Remote Access Services (RAS). You can add users to the VPN just as you add devices, enabling user access to all resources within the VPN.
About Route-Based VPNs

Like a policy-based VPN, a route-based VPN tunnels traffic between two security devices, or between one security device and a remote user. However, a route-based VPN automatically tunnels all traffic between two termination points, without regard for the type of traffic. Because the tunnel is an always-on connection between two network points, the security device views the tunnel as a static network resource through which to route traffic.

To create the termination points of the tunnel, you designate an interface on the security device as a tunnel interface, then define a static route or use a dynamic routing protocol (BGP, OSPF) between all tunnel interfaces in the VPN. The tunnel interface, just like a physical interface, maintains state to enable dynamic routing protocols to make route decisions. When using VPN Manager to create your route-based VPN, the tunnel interfaces are automatically created for you.

VPN Checklist

After you have carefully considered your VPN requirements, create a VPN checklist to help you determine the VPN components you need to create. You might also want to create a network diagram of your topology that includes protected resources, VPN members, their IP addresses and gateways, and the type of tunnel between them.

Define Members and Topology

What do you want to connect?

- Devices
- Network Components/Protected Resources
- Remote Access Service (RAS) Users
- Extranet Devices

How do you want to connect the VPN members?

- Site to Site
- Hub and Spoke
- Full Mesh

You might want to create a network diagram to map out your VPN visually, with IP addresses, to help you configure your topology.

Define VPN Type: Policy-Based, Route-Based, or Mixed-Mode

What type of traffic do you want to protect?

- Use a policy-based VPN to encrypt and authenticate certain types of traffic between two network nodes.
Use a route-based VPN to encrypt and authenticate all traffic between two network nodes.

Use a mixed-mode VPN to encrypt and authenticate traffic between policy-based and route-based VPN nodes.

Define Security Protocol (Encryption and Authentication)
How do you want to protect the VPN traffic?

- Autokey IKE
- L2TP
- L2TP over AutoKey IKE
- Manual Key (you cannot use VPN Manager to create a Manual Key VPN)

You must also decide if you want to use certificates to authenticate communication between the VPN members.

Define Method: VPN Manager or Device-Level?
How do want to create the tunnel? Using VPN Manager or configuring each device?

Using VPN Manager
When adding a VPN using the VPN Manager, you enter the VPN members, gateways, IKE properties, and VPN topology, then autogenerate the VPN rules that create the VPN. You can inspect the VPN rules and override any VPN property before sending the VPN configuration to your devices.

Choose the VPN type that best matches your VPN requirements:

- Autokey IKE VPN—Use to authenticate and encrypt traffic between devices and/or protected resources. An Autokey IKE VPN supports:
  - Mixed-mode VPNs (policy-based members and route-based members)
  - Policy-based VPNs
  - Route-based VPNs
  - ESP and AH Authentication
  - ESP AutoKey IKE Encryption
  - IP traffic
  - Tunnels between devices (routing-based) and protected resources (policy-based)

- Autokey IKE RAS VPN—Use to authenticate and encrypt traffic between remote users and protected resources. An Autokey IKE RAS VPN supports:
Planning for Your VPN

Chapter 10: Configuring VPNs

- Policy-based VPNs
- ESP and AH Authentication
- ESP AutoKey IKE Encryption
- IP traffic
- Remote access users

- L2TP RAS VPN—Use to authenticate (but not encrypt) PPP or other non-IP traffic between RAS users and protected resources. An L2TP RAS VPN supports:
  - Policy-based VPNs
  - AH Authentication
  - PPP or other non-IP traffic
  - Remote access users

- L2TP over Autokey IKE RAS VPN—Use to authenticate and encrypt PPP traffic between remote users and protected resources. An L2TP over Autokey IKE RAS VPN supports:
  - Policy-based VPNs
  - ESP and AH Authentication
  - ESP AutoKey IKE Encryption
  - PPP or other non-IP traffic
  - Remote access users

Creating Device-Level VPNs
You can create the following VPN types:

- AutoKey IKE VPN
- Manual Key IKE VPN
- L2TP VPN
- Redundant Site-Site VPN
Preparing VPN Components

After you have determine how you want to configure your VPN, you can being preparing the VPN components necessary to create the VPN. A VPN combines device-level components (such as devices, zones, and routes) with network-level components (authentication, users, and NAT) to create a secure system of communication. Before you can create a VPN, you must first configure the components that comprise the VPN.

Each VPN type has basic, required, and optional components:

- Preparing Basic VPN Components
- Preparing Required Policy-Based VPN Components
- Configuring Required Routing-Based VPN Components
- Configuring Optional VPN Components

For mixed-mode VPNs, you must configure all basic and required policy- and route-based components.

NOTE: For step-by-step instructions on creating VPNs, see the NetScreen-Security Manager Online Help topic “VPNs”.

Preparing Basic VPN Components

To create any type of VPN, ensure that all security devices you want to use in the VPN are managed by NetScreen-Security Manager and configured correctly.

- Devices—Add the security devices you want to include in the VPN to NetScreen-Security Manager, ensuring that all devices are in the same domain. If you need to add a device to a VPN in a different domain, you must add the device as an extranet device in the domain that contains the VPN, then add the extranet device to the VPN. For details on adding devices, importing devices, or using extranet devices in VPNs, see “Domain selection is critical when using VPNs. You can create VPNs only between devices within the same domain. If you need to add a device to a VPN in a different domain, add the device as an extranet device in the domain that contains the VPN, then add the extranet device to the VPN (as shown in Figure 13).” on page 79.

- Zones—Configure each security device with at least two zones (trust and untrust); each zone must contain at least one interface (physical or virtual). For details on creating and configuring zones and interfaces, see Chapter 5, “Configuring Devices”.

Preparing Required Policy-Based VPN Components

A policy-based VPN requires several components:

- Address Objects
- Protected Resources
The following sections detail how to configure each component; after you have created a component, you can use it to create your VPN.

Configuring Address Objects
You must create address objects to represent your network components in the UI. For details on creating and configuring address objects, see “Configuring Address Objects” on page 444.

Configuring Protected Resources
You should determine your protected resources first to help you identify the devices you need to include in the VPN. After you know what you want to protect, you can use VPN Manager or manually configure your security devices to create the VPN. A protected resource object represents the network components (address objects) and services (service objects) you want to protect and the security device that protects them.

The address specifies secured destination, the service specifies the type of traffic to be tunneled, and the device specifies where the VPN terminates (typically an outgoing interface in untrust zone). In a VPN rule, protected resources are the source and destination IP addresses.

When creating protected resources:
- To protect multiple network components that are accessible by the same security device, add the address objects that represent those network components to the protected resource object.
- To protect a single network component that is accessible by multiple security devices, add multiple devices to the protected resource object. You must configure each device to be a part of the VPN.
- To manage different services for the same network component, create multiple protected resource objects that use the same address object and security device but specify a different service object.
- If you change the security device that protects a resource, NetScreen-Security Manager removes the previous security device from all affected VPNs and adds the new security device. However, NetScreen-Security Manager does not configure the VPN topology for the new security device—you must reconfigure the topology to include the new device manually.

For more details on creating protected resources, see “Configuring Protected Resources” on page 520.

Configuring Shared NAT Objects
For VPNs that support policy-based NAT, you must create one or more shared NAT objects. A shared NAT object contains references to device-specific NAT objects, enabling multiple devices to share a single object.
First, create a device-specific NAT object by editing the device configuration of each security device member. Then, create a global NAT object that includes the device-specific NAT objects. In the Object Manager, create a single shared NAT object to represent similar device-specific NAT objects (for example, a global DIP represents multiple device-specific DIPs). Use the global NAT object in your VPN; when you install the VPN on a device, that device automatically replaces the shared NAT object with its device-specific NAT object.

For details on shared NAT objects, see “Configuring NAT Objects” on page 516.

Configuring Remote Access Service (RAS) Users
For VPNs that support RAS users, you must create a User Object to represent each user. NetScreen-Security Manager supports two types of users:

- **Local Users**—A local user has an account on the security device that guards the protected resources in the VPN. When a local user attempts to connect to a protected resource, the security device authenticates the user.

- **External Users**—An external user has an account on RADIUS or SecureID Authentication Server. When an external attempts to connect to a protected resource, the security device forwards the request to the authentication server for authentication.

**Authenticating RAS Users**
You can authenticate/encrypt a RAS user using one or more of the following protocols:

- **XAuth**—Uses IPSec ESP and a username and password for authentication. XAuth RAS users must authenticate with a username and password when they connect to the VPN tunnel.

- **AutoKey IKE**—Uses IPSec ESP and AH for encryption and authentication. AutoKey IKE users have a unique IKE ID that NetScreen-Security Manager uses to identify and authenticate the user during IKE Phase I negotiations. To simplify RAS management for large numbers of AutoKey IKE users, you can also create AutoKey IKE groups that use a shared Group IKE ID.

- **L2TP**—Uses Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP) for authentication (password sent in the clear).

- **Manual Key IKE**—Uses IPSec ESP and AH for encryption and authentication. Because manual key users are device-specific, you create them in the security device configuration, not in the Object Manager. For details on creating manual key users, see “Configuring L2TP and XAuth Local Users” on page 349.

NetScreen-Security Manager allows certificate with DC in certificate DN to be used for dialup user IKE ID selection.

When you use certificate DN as dialup user IKE ID, the following takes place:

**NOTE:**  We strongly recommend that you do not use null AH with ESP.
- On the device server, a partial or whole DN is associated with a VPN configuration.

- On the client side, the certificate DN is sent as IKE ID for the server to match the VPN configuration based on the content of DN.

The server DN configuration can contain a container part and a wildcard part as follows:

- The container part contains a continuous section of the DN, eg. “OU=a,O=b”. Any DN containing all specified elements in correct order are accepted.

- Up to seven wildcards can be specified, one for each of the following element: CN, OU, O, L, ST, C, Email.

NetScreen-Security Manager needs to support DC container type when using ASN1-DN to create IKE ID or a group of IKE ID that enables multiple, concurrent connections to the same VPN tunnel. During Phase 1 negotiations, IKE first attempts to make an exact match between the RAS IKE ID and peer gateway IKE ID.

If no match is found, IKE then attempts to make a partial match between the RAS IKE ID and Group IKE ID. When selecting this type, you must enter a container identity or a wildcard ID (CN, OU, O, L, ST, C, Email).

NetScreen-Security Manager devices authenticate a RAS IKE user's ID if the values in the RAS IKE user's ASN1-DN identity fields exactly match the values in the group IKE user's ASN1-DN identity fields. The container ID type supports multiple entries for each identity field (for example, "ou= eng,ou= sw,ou= screenos"). The ordering of the values in the identity fields of the two ASN1-DN strings must be identical. In this IKE ID matching part, we need to allow DC element to be matched.

NetScreen-Security Manager also supports DC in wildcard when using ASN1-DN to create IKE ID or a group of Wildcard ID.

NetScreen-Security Manager devices authenticate a RAS IKE user's ID if the values in the RAS IKE user's ASN1-DN identity fields match those in the group IKE user's ASN1-DN identity fields. The wildcard ID supports only one value per identity field (for example, "ou= eng" or "ou= sw", but not "ou= eng, ou= sw"). The ordering of the identity fields in the two ASN1-DN strings are inconsequential. In this IKE ID matching part, we need to support DC as a wildcard element.

**Configuring Group IKE IDs**

If your VPN includes multiple remote users, it can be impractical to create an IKE ID and VPN rule for each. Instead, you can use a Group IKE ID to authenticate multiple users in a single VPN rule. In the security device configuration VPN settings, create a VPN Group and specify the maximum number of concurrent connections that the group supports (cannot exceed the maximum number of allowed Phase 1 SAs or the maximum number of VPN tunnels allowed on the Juniper Networks security device platform).

For details on group IKE IDs, see the ScreenOS 5.x Concepts and Examples Guide.
Configuring Required Routing-Based VPN Components

A route-based VPN requires two components:

- Tunnel Interface or Zone
- Route (Static or Dynamic)

The following sections detail how to configure each required component.

For VPNs created with VPN Manager, you create the VPN first to autogenerate the tunnel interfaces, then create the routes on the device itself using those tunnel interfaces. For VPNs created at the device level, you can create the tunnel interfaces and routes before or after configuring the VPN.

Configuring Tunnel Interfaces and Tunnel Zones

A VPN requires a physical or virtual interface on the security device, and each security device supports a specific number of physical and virtual interfaces. To support multiple VPNs on a device, you might want to create tunnel interfaces and tunnel zones to increase the number of available interfaces on the device.

NOTE: VPN Manager automatically creates the necessary tunnel interfaces for route-based VPNs. For device-level VPNs, you can create the tunnel interfaces before or after creating the VPN.

If you do not need to do address translation (NAT), use unnumbered.

- Tunnel Interfaces—A tunnel interface handles VPN traffic between the VPN tunnel and the protected resources. You can create numbered tunnel interfaces that use unique IP addresses and netmasks, or unnumbered tunnel interfaces that do not have their own IP address and netmask (unnumbered tunnel interface borrows the IP address of the default interface of the security zone).

- Tunnel Zones—A tunnel zone is a logical construction that includes one or more numbered tunnel interfaces. You must bind the VPN tunnel to the tunnel zone (not the numbered tunnel interfaces); the VPN tunnel uses the default interface for the tunnel zone. In a policy-based VPN, you can link:
  - A single VPN tunnel to multiple tunnel interfaces
  - Multiple VPN tunnels to a single tunnel interface

For details on tunnel interfaces and tunnel zones, see “Configuring a Tunnel Interface” on page 258.
Configuring Static and Dynamic Routes

A security device must know the path, or route, between each protected resource or security device in the VPN before it can forward packets from the source network to the destination network on the other side of the tunnel. To specify the route, you can use static routes, which define a specific, unchanging path between two VPN nodes, or dynamic routes, which define an algorithm that dynamically determines the best path between two VPN nodes.

NOTE: If you are using VPN Manager to create the route-based VPNs, you create the routes after autogenerating the VPN. If you are creating a device-level VPN, you can create the routes after configuring the tunnel interfaces.

To create a static route, you must manually create a route for each tunnel on each device. For VPNs with more than just a few devices, Juniper Networks highly recommends using a dynamic routing protocol to automatically determine the best route for VPN traffic:

To route between different networks over the Internet, use Border Gateway Protocol (BGP); to route within the same network, use Open Shortest Path First (OSPF). For details on creating routes, see “Configuring Virtual Routers” on page 169.

Configuring Optional VPN Components

In any type of VPN, you can also use three optional components:

- Authentication Server
- Certificate and Certificate Revocation List Objects
- PKI Defaults

The following sections detail how to configure each optional component; after you have created the component, you can use it to create your VPN.

Creating Authentication Servers

To externally authenticate VPN traffic for XAuth and L2TP, you must create an authentication server object to use in your VPN. For details on authentication servers, see “Configuring Authentication Servers” on page 498.

Creating Certificate Objects

To authenticate external devices, use a Group IKE ID to authenticate multiple RAS users, or provide additional authentication for the security devices in your VPN, you must obtain and install a digital certificate on each VPN member. A digital certificate is an electronic means for verifying identity through the word of a trusted third party, known as a Certificate Authority (CA). The CA is a trusted partner of the VPN member using the digital certificate as well as the member receiving it.

The CA also issues certificates, often with a set time limit. If you do not renew the certificate before the time limit is reached, the CA considers the certificate inactive. A VPN member attempting to use an expired certificate is immediately detected (and rejected) by the CA.
To use certificates in your VPN, you must configure:

- **Local Certificate**—Use a local certificate for each security device that is a VPN member.

- **Certificate Authority (CA) Object**—Use a CA object to obtain a local and CA certificate.

- **Certificate Revocation List (CRL) Object**—Use a CRL object to ensure that expired certificates are not accepted; a CRL is optional.

### Configuring Local Certificates

A local certificate validates the identity of the security device in a VPN tunnel connection. To get a local certificate for a device, you must prompt the device to generate a certificate request (includes public/private key pair request) using the Generate Certificate Request directive. In response, the device provides certificate request that includes the encrypted public key for the device. Using this encrypted public key, you can contact an independent CA (or use your own internal CA, if available) to obtain a local device certificate file (.cer file).

You must install this local certificate file on the managed device using NetScreen-Security Manager before you can use certificates to validate that device in your VPN. Because the local certificate is device-specific, you must use a unique local certificate for each device.

You can also use SCEP to configure the device to automatically obtain local certificate (and a CA certificate) from the CA directly. For details on local certificates, see “Configuring A Local Certificate” on page 367.

### Configuring CA Objects

A CA certificate validates the identity of the CA that issued the local device certificate. You can obtain a CA certificate file (.cer) from the CA that issued the local certification, then use this file to create a Certificate Authority object.

You must install this CA certificate on the managed device using NetScreen-Security Manager before you can use certificate to validate that device in your VPN. Because the CA certificate is an object, however, you can use the same CA for multiple devices, as long as those devices use local certificates that were issued by that CA.

You can also use SCEP to configure the device to automatically obtain a CA certificate at the same time it receives the local certificate. For details on configuring a certificate authority object, see “Configuring Certificate Authorities” on page 517.

### Configuring CRL Objects

A Certificate Revocation List (CRL) identifies invalid certificates. You can obtain a CRL file (.crl) from the CA that issued the local certification and CA certificate for the device, then use this file to create a Certificate Revocation object.

You must install the CRL on the managed device using NetScreen-Security Manager before you can use a CRL to check for revoked certificates in your VPN. Because the CRL is an object, however, you can use the same CRL for multiple devices, as long as those devices use local and CA certificates that were issued by that CA.
After you have received a CRL list, you can use the CRL object in your VPN. For details on configuring a certificate revocation list object, see “Configuring CRL Objects” on page 520.

Creating PKI Defaults
You can configure default PKI settings for each security device that define how that device handles certificates. When configuring a VPN that includes the device, you can use these default settings. For details on PKI defaults, see “Configuring PKI Defaults” on page 373.

Creating VPNs with VPN Manager

Configuring a VPN using VPN Manager is an eight stage process:

- Adding the VPN
- Configuring Members (policy-based, RAS users, routing-based)
- Configuring Topology (AutoKey IKE only)
- Configuring Gateways
- Configuring IKE
- Autogenerating VPN Rules
- Configuring Overrides
- Adding the VPN Link

**NOTE:** For an L2TP RAS VPN, you do not need to configure gateways or IKE.

The following sections detail each step.

**NOTE:** For step-by-step instructions on creating VPNs, see the NetScreen-Security Manager Online Help topic “VPNs”.

Adding the VPN

From the menu bar, click VPN Manager > New and select the VPN type:

- AutoKey IKE VPN—Use to connect devices and/or protected resources. An AutoKey IKE VPN supports mixed-mode, policy-based, and routing-based VPNs, but does not support RAS users.

- AutoKey IKE RAS VPN—Use to connect IKE RAS users and protected resources. An Autokey IKE RAS VPN supports policy-based VPNs and IKE RAS users, but does not support routing-based VPNs, mixed-mode VPNs, or L2TP RAS users.

- L2TP RAS VPN—Use to connect L2TP RAS users and protected resources without encryption.
- L2TP over AutoKey IKE RAS VPN—Use to connect L2TP RAS users and protected resources. An L2TP over AutoKey IKE RAS VPN supports policy-based VPNs and L2TP RAS users, but does not support routing-based or mixed-mode VPNs.

Enter a name for the VPN, then specify the general properties for the VPN:

- **Enable**—Use this option to enable/disable the VPN. If you disable the VPN, the autogenerated VPN rules, VPN member gateways, and other device configuration settings are not installed on your managed devices.

- **Termination Point**—Select the Default Zone for the VPN Termination Point. Typically, the default zone is untrust. When you configure the topology for the VPN, you can select a unique termination point for each VPN member.

- **View Properties**—Configure the VPN components that the VPN Manager displays for the VPN:
  
  - **Type (AutoKey IKE VPN Only).** Select the components you want to configure for the VPN: Route-based components, Policy-based components, or both. By default, VPN Manager displays all Route- and Policy-based components for an AutoKey IKE VPN.
  
  - **Dial Backup.** When enabled, VPN Manager displays the dial backup option for route-based components (dial backup is supported only on NetScreen-5GT devices running ScreenOS 5.1 and higher).

Click OK to save the VPN and return to VPN Manager.

**Configuring Members**

The second step in configuring your VPN is to add members to the VPN. Depending on the type of VPN you are creating, you can add protected resources, security devices, and/or RAS users as VPN members.

**Adding Policy-Based Members**

In policy-based configuration area, you can add protected resources to the VPN. Click Protected Resources link and select the predefined Protected Resources you want to include in the VPN. For details on creating Protected Resources, see “Configuring Protected Resources” on page 520.

After you have added the protected resources, you can configure NAT and/or L2TP settings on the security device that protects each resource:

- For L2TP RAS VPNs and L2TP over AutoKey IKE VPN protected resources, you must configure L2TP settings.

- For all protected resources, you can configure policy-based NAT. Use policy-based NAT to translate private source IP addresses to Internet-routeable IP addresses. Configuring NAT is optional; if you do not use NAT on your network, you do not need to configure NAT for the VPN.

The following sections detail how to configure NAT and L2TP.
Configuring NAT

Below the Protected Resources window, select NAT to display the protecting security devices for each protected resource. Select the device for which you want to configure NAT. Enable NAT and specify the following values (you cannot edit the name of the device or the zone that contains the protected resource).

- **Configure Incoming DIP**—You can enable the security device to use a Dynamic IP pool for incoming VPN traffic. For each incoming VPN packet, the device translates the destination address into a IP address that is selected from the DIP pool.
  - Interface for Incoming DIP. Select the interface that receives traffic addressed to Dynamic IP addresses.
  - Incoming Global DIP. Select the Global DIP object that represents range of IP addresses available to the security device. (This DIP pool must include IP addresses that are routeable on your internal network.)

For details on configuring DIP objects, see “Configuring DIP Objects” on page 516.

- **Configure Tunnel Interface and Zone**—You can bind the VPN tunnel to a tunnel interface or tunnel zone to increase the number of available interfaces in the security device.
  - Tunnel Zone. Select a pre-configured tunnel zone on the security devices to bind the VPN tunnel directly to the tunnel zone. The tunnel zone must include one or more numbered tunnel interfaces; when the security devices route VPN traffic to the tunnel zone, the traffic uses one or more of the tunnel interfaces to reach the protected resources.
  - Tunnel Interface. Select a pre-configured tunnel interface on the security devices to bind the VPN tunnel to the tunnel interface. The security devices route all VPN traffic through the tunnel interface to the protected resources.

**NOTE:** If the security device is running ScreenOS 5.x and configured in transparent mode, you can only configure the zone (the interface does not appear) ScreenOS 4.0.x devices display both zone and interface.

To use a tunnel interface and/or tunnel zone in your VPN, you must first create the tunnel interface or zone on the device; for details, see “Configuring Tunnel Interfaces and Tunnel Zones” on page 608 and “Configuring a Tunnel Interface” on page 258.

- Tunnel Zone. Select a pre-configured tunnel zone on the security devices to bind the VPN tunnel directly to the tunnel zone. The tunnel zone must include one or more numbered tunnel interfaces; when the security devices route VPN traffic to the tunnel zone, the traffic uses one or more of the tunnel interfaces to reach the protected resources.
- Tunnel Interface. Select a pre-configured tunnel interface on the security devices to bind the VPN tunnel to the tunnel interface. The security devices route all VPN traffic through the tunnel interface to the protected resources.

- **Configure MIP, VIP, and Outgoing DIP**
  - Enable MIP. Enable MIP to use a mapped IP address for the interface.
  - Global MIP. Select the global MIP object that represents the mapped IP address you want to use for the interface.
  - Global VIP. Select the global VIP object that represents the virtual IP address you want to use for the interface.
Global DIP (Outgoing). You can enable the security device to use a Dynamic IP pool for outgoing VPN traffic. For each outgoing VPN packet, the device translates the source address into a IP address selected from the DIP pool. Select the Global DIP object that represents range of IP addresses available to the security device. (This DIP pool must include IP address that are routeable on the Internet.)

Configuring L2TP
For L2TP RAS VPNs and L2TP over AutoKey IKE VPN protected resources, you must configure L2TP settings.

To connect to an L2TP VPN tunnel, the L2TP RAS user uses the IP address and WINS/DNS information assigned by the user’s ISP. However, when the L2TP RAS user sends VPN traffic through the tunnel, the security device assigns a new IP address and WINS/DNS information that enables the traffic to reach the destination network.

Below the Protected Resources pane, select L2TP/NAT to display the protecting security devices for each protected resource. (If you are configuring an AutoKey IKE VPN or AutoKey IKE RAS VPN, this option does not appear.) Select the device for which you want to configure L2TP. In the L2TP tab, specify the following values (you cannot edit the name of the device).

- **Host Name**—Enter the name of the L2TP host.
- **Keep Alive**—The number of seconds a VPN member waits between sending hello packets to an L2TP RAS user.
- **Peer IP**—Enter the IP address of the L2TP peer.
- **Secret**—Enter the shared secret that authenticates communication in the L2TP tunnel.
- **Remote Settings**—Select the remote settings object that represents the DNS and WINS servers assigned to L2TP RAS users after they have connected to the tunnel.
- **IP Pool Name**—Select the IP pool object that represents the available IP addresses that can be assigned to L2TP RAS users after they have connected to the tunnel.
- **Auth Server**—Because the L2TP must authenticate L2TP users, use custom settings to associate those users with a specific Authentication Server. You can also configure the device to query the remote settings object for DNS and WINS information for those users.

To use the default authentication server for L2TP users, add the users to the device first.

**NOTE:** When configuring a VPN that includes RAS users, if you added the user as a L2TP local user and assigned an IP pool and remote settings object on a specific device in the VPN, those settings override the settings defined in the VPN.
Adding RAS Users

In the Remote User area, you can add RAS users to the VPN. (When configuring an AutoKey IKE VPN, this area does not appear.) Click the Users link to display the user selection dialog box, then click the Edit icon to select the predefined RAS users or user groups you want to include in the VPN. For details on creating RAS users and groups, see “Configuring User Objects” on page 507.

Defining a Default Gateway

You can include a single RAS user in multiple VPNs. To specify this VPN as the default entry point for all RAS users listed in the VPN, enable Use as Default Gateway.

Adding Routing-Based Members

In the routing-based configuration area, you can add routing-based members to the VPN. (When configuring an AutoKey IKE RAS VPN, an L2TP RAS VPN, or an L2TP over AutoKey IKE RAS VPN, this area does not appear.) A routing-based VPN member is a security device that will route traffic (statically or dynamically) through a tunnel interface to one or more VPN members.

VPN Manager automatically creates the necessary tunnel interfaces for each route-based VPN member. However, after VPN Manager autogenerates the VPN tunnels, you must configure static or dynamic routes on the security devices to route traffic through these tunnel interfaces. For details on creating routes, see “Configuring Virtual Routers” on page 169.

Click the security devices link to display the route-based member selection dialog box.

- Configure Tunnel Interface Settings—Select a Primary Zone, Secondary Zone, and physical source interface for each security device. The selected zone passes VPN traffic through the selected interface on the security device.
  - The Zone settings apply to all route-based members selected in the members window.
  - If the Primary Zone is not defined or available on the security device, VPN traffic automatically uses the Secondary Zone.
  - The Physical Source Interface is the default physical interface on the device that transmits VPN traffic.

- Configure Tunnel Options—ScreenOS 5.x devices support additional functionality for handling VPN tunnels:
  - To use a single tunnel interface on each device for VPN traffic, enable Generate Single Tunnel Interface for 5.x devices. When enabled, the security device uses the route table and the next-hop tunnel binding table to link a specific destination to one of a number of VPN tunnels bound to the same tunnel interface. By mapping the next-hop gateway IP address specified in the route table entry to a specific VPN tunnel in the NHTB table, the device can use one tunnel interface for all VPN traffic through the device. This option is enabled by default.
To create entries in the Next Hop Tunnel Binding (NHTB) table, enable Generate NHTB entries for 5.x devices. When this option is selected, VPN Manager autogenerates NHTB entries for each VPN tunnel. **If you are using a single interface for all VPN traffic on the device but you do not select this option, you must manually add the NHTB routes in the NHTB table, or configure BGP to automatically create the entries for you.** This option is disabled by default.

For details on working with the NHTB routing table, see the Juniper Networks ScreenOS 5.x Concepts and Examples Guide, Volume 7, “Advanced VPN Features”.

Select Dial Backup to enable NetScreen-5GT security devices to use the serial port as a backup termination point for the VPN tunnel. When this option is enabled, VPN Manager automatically generates the termination point for the serial interface during VPN creation (you do not need to select the serial interface manually when configuring Termination Points).

Configure Members—Click the Add icon to select the predefined security devices you want to include in the VPN. After you have added the device to the VPN, you can double-click the device and configure overrides for the default tunnel interface zone, the physical source interface. For ScreenOS 5.x devices, you can also enable/disable single tunnel interface and NHTB entries.

After VPN Manager generates the tunnel interfaces, you must configure static or dynamic routes on each VPN member to route traffic to other VPN members.

**Configuring Topology**

In the general configuration area, you can define the topology and/or termination points of the VPN:

- The topology of the VPN determines how VPN members logically connect to each other. The topology is the communication path that VPN traffic must take to reach a VPN member.

- The termination points of the VPN determine how VPN members physically connect to each other. A termination point is the interface on each VPN member that sends and receives VPN traffic to and from the VPN tunnel.

**NOTE:** If you change the security device that protects a resource, NetScreen-Security Manager removes the previous security device from all affected VPNs and adds the new security device. However, NetScreen-Security Manager does not configure the VPN topology for the new security device—you must reconfigure the topology to include the new device manually.

For AutoKey IKE VPNs, you must define the topology for the VPN. Each VPN member is a node that has specific connection capabilities, and the topology describes the logical connections between those nodes.

A node can be:

- Hub—A hub can connect to a branch or main.
Main—A main can connect to a hub, branch, or another main. When configuring a VPN that uses multiple mains, you can select to mesh all mains (all mains can communicate with each other) or disable all main meshing.

Branch—A branch can connect to a hub or a main. Branches can send and receive VPN traffic to and from a hub or a main device, but cannot communicate directly with other branches.

Additionally, you can use a supernet to reduce the number of rules required for the hub device in a policy-based VPN. A supernet is a Address Object Group containing the network Address Objects that represent the source and destination points of the VPN. Use a supernet when the hub device supports a small number of rules.

Configuring Common VPN Topologies
You can use VPN Manager to configure the following common VPN topologies:

- **Hub and Spoke**—Select a device to act as the hub; this device connects VPN members and enables them to communicate. Next, select the VPN members to be the spokes. You are not required to use a VPN member as a hub:
  - If do not select a VPN member as the VPN hub, the hub simply routes VPN traffic from one branch to another.
  - If you do select a VPN member as the VPN hub, the hub routes VPN traffic from itself and all connected branches.

  Each spoke can send and receive VPN traffic to and from the hub, but cannot communicate directly with other spokes.

  **NOTE:** You can select only one hub per VPN.

- **Main and Branch**—Main and branch topologies combine the flexibility of hub and spoke with the redundancy of full mesh. Because you can select multiple mains, each branch has an alternate tunnel to use if one main fails. To create a main and branch:
  - Select the devices to act at mains; these devices can communicate with all other VPN members.
  - Select remaining devices as branches; these devices communicate with all mains.

- **Full Mesh**—Select all VPN members to act as mains. All members can communicate with any other VPN member. Do not select a hub.

- **Site to Site**—Select both VPN members as mains. Each member can communicate with the other VPN member. Do not select a hub.
Defining Termination Points
You must define the termination interface for each security device in the VPN. The Termination Points tab displays the default termination points for the VPN. A termination point is the interface on a security device that sends and receives VPN traffic to and from the VPN tunnel, and is typically in the Untrust zone. Each VPN member (the security devices included as routing-based members and/or as protected resources for policy-based members) has a default termination interface.

NOTE: You do not need to select the serial interface on a NetScreen-5GT security device to enable dial backup for the VPN tunnel. If you have enabled Dial Backup for the device in the Route-Based Configuration area, VPN Manager automatically generates the termination point for the serial interface during VPN creation.

To override the default termination interface, right-click the VPN member, select Edit, and select a new termination interface for the device.

Configuring Gateways
To configure the gateways for VPN, click the Gateway Parameters link.

Configuring Gateway Properties
In the Properties tab, specify the following gateway values.

Selecting a Mode
The mode determines how Phase 1 negotiations occur. Select the mode that meets your VPN requirements:

- **Main mode**—The IKE identity of each node is protected. Each node sends three two-way messages (six messages total); the first two messages negotiate encryption and authentication algorithms that protect subsequent messages, including the IKE identity exchange between the nodes. Depending on the speed of your network connection and the encryption and authentication algorithms you use, main mode negotiations can take a long time to complete. Use Main mode when security is more important.

- **Aggressive mode**—The IKE identity of each node is not protected. The initiating node sends two messages and the receiving node sends one (three messages total); all messages are sent in the clear, including the IKE identity exchange between the nodes. Because Aggressive mode is typically faster but less secure than Main mode, use Aggressive mode when speed is more important than security.

For RAS VPNs, you **must** use Aggressive mode; for VPNs that do not include RAS users, select the mode that meets your requirements.

Configuring Heartbeats
Use heartbeats to enable redundant gateways.

- **Hello**—Enter the number of seconds the security devices wait between sending hello pulses.
Reconnect—Enter the maximum number of seconds the security devices wait for a reply to the hello pulse.

Threshold—Enter the number of seconds that the security devices wait before attempting to reconnect.

Configuring NAT Traversal

Because NAT obscures the IP address in some IPSec packet headers, VPN nodes cannot receive VPN traffic that passes through an external NAT device. To enable VPN traffic to traverse a NAT device, you can use NAT Traversal (NAT-T) to encapsulate the VPN packets in UDP. If a VPN node with NAT-T enabled detects an external NAT device, it checks every VPN packet to determine if NAT-T is necessary.

Because checking every packet impacts VPN performance, you should only use NAT Traversal for remote users that must connect to the VPN over an external NAT device. You do not need to enable NAT-T for your internal security device nodes that use NAT; each VPN node knows the correct address translations for VPN traffic and does not need to encapsulate the traffic.

To use NAT-T, enable NAT-Traversal and specify:

- UDP Checksum—A 2-byte value (calculated from the UDP header, footer, and other UDP message fields) that verifies packet integrity. You must enable this option for NAT devices that require UDP checksum verification; however, most NAT devices (including security devices) do not require it.

- Keep alive Frequency—The number of seconds a VPN node waits between sending empty UDP packets through the NAT device. A NAT device keeps translated IP addresses active only during traffic flow, and invalidates unused IP addresses. To ensure that the VPN tunnel remains open, you can configure the VPN node to send empty “keep alive” packets through the NAT device.

Configuring XAuth

Use the XAuth protocol to authenticate RAS users with an authentication token (such as SecureID) and to make TCP/IP settings (IP address, DNS server, and WINS server) for the peer gateway.

- Default Server—To use the default XAuthentication server for the device. To change or assign a default XAuthentication server, edit the VPN settings in the security device configuration.

- XAuth Server—Use when the remote gateway is a security device that you want to assign TCP/IP settings.
  - Auth Server Name. Select a pre-configured authentication server object. For details on creating an authentication server object, see “Configuring Authentication Servers” on page 498.
  - Allowed Authentication Type. Select Generic or Challenge Handshake Authentication Protocol (CHAP) (password is sent in the clear) to authenticate the remote gateway.
Query Remote Setting. Enable this option to query the remote settings object for DNS and WINS information.

NOTE: When configuring a VPN that includes RAS users, if you added the user as a L2TP or XAuth local user and assigned a remote settings object on a specific device in the VPN, those settings override the settings defined in the VPN.

- XAuth Client—Use when the remote gateway is a RAS user that you want to authenticate.
  - Allowed Authentication Type. Select Any or CHAP.
  - User Name and Password. Enter the user name and password that the RAS user must provide for authentication.

NOTE: All passwords handled by NetScreen-Security Manager are case-sensitive.

- Bypass Authentication to permit VPN traffic from VPN members to pass unauthenticated by the XAuth server.

Configuring Gateway Security

Determine the authentication mechanisms you want the VPN nodes to use for IKE Phase I negotiations. You can use a preshared key or certificates for authentication.

Preshared Key/Certificate

For Phase 1, select a Preshared Key Information or PKI Information:

- Preshared Key—Use if your VPN includes security devices and/or RAS users. VPN nodes use the preshared key during Phase 1 negotiations to authenticate each other; because each node knows the key in advance, negotiations use fewer messages and are quicker.
  - To generate a random key, enter a value for the seed, then click Generate Key. NetScreen-Security Manager uses the seed value to generate a random key, which is used to authenticate VPN members.

NOTE: Using a random key can generate a key in excess of 255 characters, which exceeds ScreenOS limits and might not be accepted by the security device during update. To reduce the key size, shorten the autogenerated key value by deleting characters.

- To use a predefined value for the key, enter a value for the Preshared Key.

- PKI—Use if your VPN includes extranet devices or you require the additional security provided by certificates (PKI uses certificates for VPN member authentication). For details on creating and managing certificates, see “Configuring Certificate Authorities” on page 517.

For Phase 1, select a proposal or proposal set. You can select from predefined or user-defined proposals:
To use a predefined proposal set, select one of the following:

- Basic (nopfs-esp-des-sha, nopfs-esp-des-md5)
- Compatible (nopfs-esp-3des-sha, nopfs-esp-3des-md5, nopfs-esp-des-sha, nopfs-esp-des-md5)
- Standard (gs-esp-3des-sha, gs-esp-aes128-sha)

**NOTE:** You cannot use a predefined proposal set with certificates—you must select a user-defined proposal or change the authentication method to Preshared Key.

To use a user-defined proposal, select a single proposal from the list of predefined and custom IKE Phase 1 Proposals. For details on custom IKE proposals, see "Configuring IKE Proposals" on page 523.

If your VPN includes only security devices, you can specify one predefined or custom proposal that NetScreen-Security Manager propagates to all nodes in the VPN. If your VPN includes extranet devices, you should use multiple proposals to increase security and ensure compatibility.

**Preshared Secrets**

You can use the same preshared secret for all nodes in the VPN, or create a unique preshared secret for communication from a specific node to another node.

**Configuring IKE IDs**

Every VPN node has a unique identification number, known as an IKE ID. During Phase 1 negotiations, the IKE protocol uses the IKE ID to authenticate the VPN member.

VPN Manager automatically creates the default IKE ID for you, based on the policy- or route-based members and RAS users, so you do not need to configure this option. However, if you do not want to use the default IKE ID, you can select a different IKE ID type and configure an IKE ID for each VPN gateway.

The IKE ID tab displays all security devices included as routing-based members and/or as protected resources for policy-based members. For each device, select the IKE ID type and enter the ID value:

- **ASN1-DN**—Abstract Syntax Notation, version 1 is a data representation format that is non-platform specific; Distinguished Name is the name of the computer. Use ASN1-DN to create a Group IKE ID that enables multiple, concurrent connections to the same VPN tunnel; use a Group IKE ID to make configuring and maintaining your VPN quicker and easier.

For details on how Group IKE IDs work, see “Configuring Group IKE IDs” on page 607. For details on determining the ASN1-DN container and wildcard values for Group IKE IDs, see the Juniper Networks ScreenOS 5.x Concepts and Examples Guide.
FQDN—Use a Fully Qualified Domain Name when the gateway is a dynamic IP address. FQDN is a name that identifies (qualifies) a computer to the DNS protocol using the computer name and the domain name; ex. server1.colorado.mycompany.com.

IP Address—Use an IP address when the gateway has a static IP address.

U-FQDN—Use a User Fully Qualified Domain Name when the gateway is a dynamic IP address, such as a RAS user. A U-FQDN is a simply an email address; ex. user1@mycompany.com.

### Configuring IKE

To configure the IKE properties and Phase 2 Proposals for the VPN, click the IKE Parameters link. Because L2TP RAS VPNs do not support encryption, you do not need to configure IKE properties for L2TP RAS VPNs.

#### IKE Properties

Configure the IKE properties:

- **Idle Time to Disable SA**—Configure the number of minutes before a session that has no traffic automatically disables the SA.

- **Replay Protection**—In a replay attack, an attacker intercepts a series of legitimate packets and uses them to create a denial-of-service (DoS) against the packet destination or to gain entry to trusted networks. If replay protection is enabled, your security devices inspect every IPSec packet to see if the packet has been received before—if packets arrive outside a specified sequence range, the security device rejects them.

- **IPSec Mode**—Configure the mode:
  - Use tunnel mode for IPSec. Before an IP packet enters the VPN tunnel, NetScreen-Security Manager encapsulates the packet in the payload of another IP packet and attaches a new IP header. This new IP packet can be authenticated, encrypted, or both.
  - Use transport mode for L2TP-over-AutoKey IKE VPNs. NetScreen-Security Manager does not encapsulate the IP packet, meaning that the original IP header must remain in plaintext. However, the original IP packet can be authenticated, and the payload can be encrypted.
  - Do not set Fragment Bit in the Outer Header—The Fragment Bit controls how the IP packet is fragmented when traveling across networks.
    - Clear. Use this option to enable IP packets to be fragmented.
    - Set. Use this option to ensure that IP packets are not fragmented.
    - Copy. Select to use the same option as specified in the internal IP header of the original packet.
Monitor

You can enable VPN Monitor and configure the monitoring parameters for the device. Monitoring is off by default. To enable the VPN Monitor in Realtime Monitor to display statistics for the VPN tunnel, configure the following:

- VPN Monitor—When enabled, the security devices in the VPN send ICMP echo requests (pings) through the tunnel at specified intervals (configurable in seconds) to monitor network connectivity (each device uses the IP address of the local outgoing interface as the source address and the IP address of the remote gateway as the destination address). If the ping activity indicates that the VPN monitoring status has changed, the device triggers an SNMP trap; the VPN Monitor (in RealTime Monitor) tracks these SNMP statistics for VPN traffic in the tunnel and displays the tunnel status.

- Rekey—When enabled, the security devices in the VPN regenerate the IKE key after a failed VPN tunnel attempts to re-establish itself. When disabled, each device monitors the tunnel only when the VPN passes user-generated traffic (instead of using device-generated ICMP echo requests). Use the rekey option to:
  - Enable dynamic routing protocols to learn routes and transmit messages through the tunnel.
  - Automatically populate the next-hop tunnel binding table (NHTB table) and the route table when multiple VPN tunnels are bound to a single tunnel interface.

For details on VPN monitoring at the device level, see the Juniper Networks ScreenOS 5.x Concepts and Examples Guide. For details on VPN Monitor (in Realtime Monitor) in NetScreen-Security Manager, see “Monitoring VPNs” on page 706.

Configuring Security Level

For Phase 2 negotiations, select a proposal or proposal set. You can select from predefined or user-defined proposals:

- To use a predefined proposal set, select one of the following:
  - Basic (nopfs-esp-des-sha, nopfs-esp-des-md5)
  - Compatible (nopfs-esp-3des-sha, nopfs-esp-3des-md5, nopfs-esp-des-sha, nopfs-esp-des-md5)
  - Standard (gs-esp-3des-sha, gs-esp-aes128-sha)

- To use a user-defined proposal, select a single proposal from the list of predefined and custom IKE Phase 2 Proposals. For details on custom IKE proposals, see “Configuring IKE Proposals” on page 523.

If your VPN includes only security devices, you can specify one predefined or custom proposal that NetScreen-Security Manager propagates to all nodes in the VPN. If your VPN includes extranet devices, you should use multiple proposals to increase security and ensure compatibility.
Autogenerating VPN Rules

When you have completed configuring the policy- and route-based VPN members, the topology (if necessary) and termination points, and the IKE (if necessary) and gateway parameters for the VPN, you are ready to autogenerate the VPN.

During autogeneration, NetScreen-Security Manager generates the VPN rules that control traffic between policy-based VPN members, and edits the device configuration (gateways, security parameters, and so on) of each VPN member to support the VPN.

Autogeneration does not:

- Insert the VPN rules into a Security Policy. After you have reviewed the VPN rules and made any necessary overrides, you must manually insert the VPN rules (known as a VPN link) into a Security Policy. For details, see “Adding the VPN Link” on page 626.

- Install the new VPN rules or edited device configurations on the managed devices in the VPN. After you have inserted the VPN link into a Security Policy, you can install that policy on your devices using the Updated directive.

- Create static or dynamic routes for route-based VPNs.

To autogenerate the VPN, click Save.

Configuring Overrides

The override area enables you configure individual settings for each VPN rules (for policy-based and mixed-mode VPNs) and each VPN member. Each change you make to the autogenerated rules or VPN member configuration is known as an override to the VPN settings.

You might need to override the VPN settings to:

- Configure additional security for specific tunnels.
- Configure additional authentication between specific VPN members.
- Configure unique monitoring or reporting options for specific VPN members or VPN tunnels.
- Configure unique IKE IDs for each VPN member.

Editing Policy Rules

For policy-based and mixed-mode VPNs, NetScreen-Security Manager automatically generates the VPN rules to control traffic between VPN members. To view these autogenerated rules, click the Policy Rules link in the Overrides area; the rules appear in a separate NetScreen-Security Manager window, using the same row and column format as in the Security Policies.

NOTE: Policy rules do not appear for route-based VPNs.
Changing Rule Position

The position of the rules indicates the order that they apply to traffic. To change the position of a rule, you can:

- Right-click the rule and select Move Rule Up or Move Rule Down, or
- Right-click the rule and select Change Rule Position. In the New Position dialog box, enter a new rule number for this rule. (The rule number is the first column in the policy table.)

Filtering Rules

You can also filter the VPN rules by zones using the Zone Filter in the upper right-hand corner of the VPN rule window. Select a zone in From Zone and/or the To Zone to order the rules as desired.

To save this rule order, click Apply.

Configuring Rule Options

You can configure rule options for each rule, including traffic shaping, logging, AntiVirus and Attack Objects, and protection actions. For details on configuring these options, see “Configuring Firewall Rule Options” on page 542.

Editing Device Configuration

For all VPNs, you can edit the device configuration for each VPN member. The device configuration displays the interfaces, gateways, and other VPN configuration information for each individual device.

Overriding Interfaces

For route-based and mixed-mode VPNs, this displays the tunnel interfaces and virtual routers configured on the VPN member. To override the general properties and dynamic routing protocols for each tunnel interface, right-click the tunnel interface and configure the settings.

For policy-based VPNs, no tunnel interfaces appear.

Overriding AutoKey IKE VPN Settings

For VPNs that use AutoKey IKE, this displays the VPN name, remote gateway, and IPSec Mode for each tunnel in the VPN. To override the general properties, security, binding/proxyID, and monitoring option for each VPN tunnel, right-click the VPN name and configure the settings as desired.
Overriding Gateways
For all VPNs, this displays the gateway name, gateway mode, IP address, and IKE phase I proposals for each VPN gateway. To override the general properties, security, and IKE ID/XAuth options for each gateway, right-click the gateway name and configure the settings as desired.

Overriding VPN Groups
For all VPNs, this displays VPN groups.

Overriding L2TP Settings
For L2TP VPNs, this displays L2TP information for each VPN member. To edit this information, right-click and configure the settings as desired.

Viewing the Device Tunnel Summary
For route-based and mixed-mode VPNs, you can view the VPN tunnels between each route-based member, including the source and peer devices, the tunnel interface, zone, and physical interface.

NOTE: The device tunnel summary does not appear for policy-based VPNs.

You cannot edit the device tunnels from this view; to make overrides to the VPN tunnels, edit the interface configuration for each device.

Adding the VPN Link
After you have reviewed the autogenerated information and made any desired overrides to the VPN, you must update your managed devices to activate the VPN. By default, the VPN you created in VPN manager is installed as the first rule in the Security Policy for each managed device. However, the Security Policy does not display the VPN.

You can manually add a VPN link to your Security Policy; a VPN link creates a link between the Security Policy and VPN (the link points to the VPN rules that exist in the VPN in VPN Manager). You might want to add a VPN link so you can reposition it elsewhere in the policy, or simply to make the VPN viewable in your policy.

To create a VPN link, in Security Policies, select an existing Security Policy (or create a new Security Policy), then right-click and select Add VPN link. Select the VPN name and click OK to add the link to the policy. By default, the link appears at the top of the policy, but you can move the VPN link anywhere in the policy, just as you would a firewall rule.

If you make changes to the VPN or create overrides, the VPN link automatically updates to reflect those edits.

Editing VPNs
To edit a VPN created with VPN Manager:
1. In the navigation tree, select VPNs. A table listing all configured VPNs appears in the main display area.

2. Right-click the VPN you want to edit and select Edit. The expanded VPN view dialog box appears.

3. Make the necessary changes, then click OK to apply your changes.

To revert any changes you have made to the VPN, right-click the VPN name in the navigation tree and select Revert Changes.

Editing VPN Protected Resources

To edit a protected resource in the VPN, right-click the protected resource and select Edit Protected Resource. Make your changes, then click OK to save your changes.

If you make changes to a protected resource object that is used in a VPN, NetScreen-Security Manager automatically generates new configuration and propagates your changes to all affected security devices. If you change the security device that protects a resource, NetScreen-Security Manager removes the previous security device from all affected VPNs and adds the new security device.

However, NetScreen-Security Manager does not configure the VPN topology for the new security device—you must reconfigure the topology to include the new device manually.

Editing Users

To edit a user object in the VPN, right-click the user and select Edit Remote User. Make your changes, then click OK to save your changes.

Editing the VPN Configuration

To add or delete a member, edit any VPN parameter, or reconfigure the VPN topology, select the VPN and click OK. Make your changes, then click Save to re-generate the VPN.

NOTE: After you click Save, you cannot revert your changes to a VPN.

Editing VPN Overrides

If you add, edit, or delete an override, the VPN link automatically updates the autogenerated rules to reflect those edits.

VPN Manager Examples

This section provides examples of common VPN types:

- Configuring an AutoKey IKE, Policy-Based Site-to-Site VPN
- Configuring an AutoKey IKE RAS, Policy-Based VPN
- Configuring an AutoKey IKE, Route-Based Site-to-Site VPN
Configuring XAuth Authentication with External User Group

The following sections provide step-by-step instructions on creating each VPN type.

**NOTE:** For examples on creating a Manual Key VPN, see “Device-Level VPN Examples” on page 665.

**EXAMPLE: CONFIGURING AN AUTOKEY IKE, POLICY-BASED SITE-TO-SITE VPN**

An AutoKey IKE VPN connects protected resources using AutoKey IKE. Use this VPN type to connect and control traffic between two security devices.

In this example, an AutoKey IKE tunnel using a pair of certificates (one at each end of the tunnel) provides the secure connection between the Tokyo and Paris offices. For the Phase 1 and 2 security levels, you specify the Phase 1 proposal as rsa-g2-3des-sha and select the predefined “Compatible” set of proposals for Phase 2. It is assumed that both participants already have RSA certificates and are using Entrust as the certificate authority (CA). All zones are in the trust-vr.

Figure 148: Configure AutoKey IKE VPN Example Overview

1. Configure the security devices. For details on adding devices, see Chapter 4, “Adding Devices”.
   a. Configure the Tokyo device with the following interfaces:
      - Ethernet1 is the Trust IP (10.1.1.1/24) in the Trust zone.
      - Ethernet3 is the Untrust IP (1.1.1.1/24) in the Untrust zone.
   b. Configure the Paris device with the following interfaces:
      - Ethernet1 is the Trust IP (10.2.2.1/24) in the Trust zone.
      - Ethernet3 is the Untrust IP (2.2.2.2/24) in the Untrust zone.
2. Create the Address Objects that you will use to create Protected Resources (for details on creating or editing Address Objects, see “Configuring Address Objects” on page 444). If you imported a security device, the address book objects configured on that device are automatically imported as Address Objects into the NetScreen-Security Manager UI.

   a. Add the Tokyo Trust LAN (10.1.1.0/24) as an network Address Object. In Address Objects, click the Add icon and select Network. Configure the following, then click OK:

      • For Name, enter Tokyo Trust LAN
      • For IP Address/Netmask, enter 10.1.1.0/24
      • For Color, select magenta.
      • For Comment, enter Tokyo Trust Zone.

   b. Add the Paris Trust LAN (10.2.2.0/24) as a network Address Object. In Address Objects, click the Add icon and select Network. Configure the following, then click OK:

      • For Name, enter Paris Trust LAN
      • For IP Address/Netmask, enter 10.2.2.0/24
      • For Color, select magenta.
      • For Comment, enter Paris Trust Zone.

3. Create the Protected Resources to represent the source and destination points of the VPN. (for details on creating or editing Protected Resources, see “Configuring Protected Resources” on page 520).

   a. Create the Tokyo Protected Resources object. In Protected Resources (under VPN Manager), click the Add icon. Configure as shown below, then click OK:
Figure 149: Create Tokyo Protected Resource Object for AutoKey IKE VPN

![Protected Resource]

b. Create the Paris Protected Resources object. In Protected Resources (under VPN Manager), click the Add icon. Configure as shown below, then click OK:

Figure 150: Create Paris Protected Resource Object for AutoKey IKE VPN

![Protected Resource]

4. Create the VPN. In the navigation tree, double-click VPN Manager, then right-click VPNs and select AutoKey IKE VPN. The New AutoKey IKE VPN dialog box appears. Configure the General VPN Properties:

a. In Name, enter Tokyo-Paris Policy-Based VPN.

b. Select Enable.

c. In Termination Point, select Untrust.

d. For VPN Type, select Policy-Based.

e. Click OK to save the VPN and return to VPN Manager.
5. Configure the policy-based members:
   a. Select the Protected Resources link to display the Protected Resources list.
   b. Select the Paris Protected Resources and the Tokyo Protected Resources.
   c. Click OK to return to the main display area.

6. Configure the VPN topology:
   a. Select the Topology link to display the Topology dialog box.
   b. Click the Add icon to display the Topology configuration dialog box. Configure the following:
      - For Hub and Supernet, leave the default of none.
      - Enable Mesh Main(s).
      - In the Mains window, select the Paris and Tokyo security devices.
   c. Click OK to return to the Topology dialog box, then click OK to return to the main display area.

7. Configure the termination points of the VPN:
   a. Click the Termination Points link. The Termination Points dialog box appears.
   b. Confirm that both Paris and Tokyo devices use a Termination Interface of ethernet3.
   c. Click OK to return to the main display area.

8. Configure the VPN gateway:
   a. Click the Gateway Parameters link. The Properties tab appears. Leave all defaults and click the Security tab.
   b. In the Security tab, configure the PKI Information and Phase 1 Proposals as shown below:
c. Click Save to save your configuration changes to the VPN.

To view the autogenerated rules, click the Policy Rules link in the Overrides section. VPN Manager generates the rules as shown below:

9. Add the VPN Link. You must create a VPN link between the Zone rulebase in a Security Policy and the VPN Manager autogenerated rules. You create this link by inserting a VPN link in the zone rulebase; this links points to the VPN rules that exist in the VPN Manager.

   a. In Security Policies, select an existing Security Policy (or create a new Security Policy). In the Zone rulebase, right-click and select Add VPN link.

   b. Select the Tokyo-Paris Policy-Based VPN, then click OK to add the link. By default, the link appears at the top of the rulebase, but you can move the VPN link anywhere in the rulebase, just as you would a firewall rule.
EXAMPLE: CONFIGURING AN AUTOKEY IKE RAS, POLICY-BASED VPN

An AutoKey IKE RAS VPN connects RAS users and protected resources. In this example, Local Auth user Wendy (login name: reporter, password: Nd4syst4) wants to access resources on the UNIX server at the corporate site.

To accommodate Wendy, create an AutoKey IKE tunnel using a preshared key to provide the secure communication channel between IKE user Wendy and the UNIX server, which is protected by the Chicago Corporate security device.

The tunnel uses ESP with 3DES encryption and SHA-1 authentication. For the Phase 1 and 2 security levels, specify the Phase 1 proposal as pre-g2-3des-sha and select the predefined “Compatible” set of proposals for Phase 2.

1. Add the Chicago Corporate device (for details on adding devices, see Chapter 4, “Adding Devices”) and configure the following interfaces:
   - Ethernet1 is the Trust IP (10.1.1.1/24) in the Trust zone.
   - Ethernet3 is the Untrust IP (1.1.1.1/24) in the Untrust zone.
2. Create the Address Objects that you will use to create Protected Resources (for details on creating or editing Address Objects, see “Configuring Address Objects” on page 444).
   a. Add the Chicago Corporate Trusted LAN (10.1.1.0/24) as an network Address Object. In Address Objects, click the Add icon and select Network. Configure the following, then click OK:
      - For Name, enter Chicago Corporate Trust LAN.
      - For IP Address/Netmask, enter 10.2.1.0/24.
      - For Color, select magenta.
      - For Comments, enter Chicago Trusted Network.
   b. Add the UNIX Server (10.1.1.5) as a host Address Object. In Address Objects, click the Add icon and select Host. Configure the following, then click OK:
3. Create Chicago Corporate Trusted LAN Protected Resources to represent the destination point of the VPN (for details on creating Protected Resources, see “Configuring Protected Resources” on page 520). In Protected Resources (under VPN Manager), click the Add icon. Configure as shown below, then click OK:

Figure 154: Add Chicago Protected Resource for AutoKey IKE RAS VPN

<table>
<thead>
<tr>
<th>Protected Resource</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Color</td>
</tr>
<tr>
<td>Service Object</td>
</tr>
<tr>
<td>Server/Client</td>
</tr>
<tr>
<td>Network Object</td>
</tr>
<tr>
<td>Comment</td>
</tr>
</tbody>
</table>

4. Create a Local User Object to represent Wendy, the remote user (for details on creating User Objects, see “Configuring User Objects” on page 507). Local User objects are authenticated with the local NetScreen-Security Manager database.

a. In User Objects, select Local User Objects. In the main display area, click the Add icon and select Local. Configure as shown below, then click OK:
5. Create the VPN. In the navigation tree, double-click VPN Manager, then right-click VPNs and select AutoKey IKE RAS VPN. The New AutoKey IKE RAS VPN dialog box appears. Configure as shown below:

   a. For Name, enter UNIX Remote Access VPN.
   b. Select Enable.
   c. In Termination Point, select Untrust.
   d. Click OK to save the VPN and return to VPN Manager. In VPN Manager, select the UNIX Remote Access VPN.

6. Configure the policy-based members:

   a. In the main display area, select the Protected Resources link.
   b. In the Protected Resources list, select the Chicago Corporate Trusted LAN, then click OK to return to the main display area.

7. Configure the termination points of the VPN:

   a. Click the Termination Points link. The Termination Points dialog box appears.
   b. Configure Chicago Corporate to use ethernet3 as the termination point (this is the Untrust interface), then click OK to return to the main display area.
8. Configure the remote users for the VPN:
   a. In the Remote Users section, click the Users link. The Remote User dialog box appears.
   b. Select the user “wparker”, then click Save to save your configuration changes to the VPN.

9. Configure the VPN gateway:
   a. Click the Gateway Parameters link. The Properties tab appears. Leave all defaults and click the Security tab.
   b. In the Security tab, enter the preshared key value (h1p8A24nG5), then click Generate Key.
   c. For Phase 1 Proposals, select User-Defined, then click the Add/Edit icon to add the pre-g2-3des-sha proposal, as shown below:

   Figure 156: Configure Security for AutoKey IKE RAS VPN

   d. Click Save to save your configuration changes to the VPN.

   To view the autogenerated rules, click the Policy Rules link in the Overrides section. VPN Manager generates the rules as shown below:

   Figure 157: View Autogenerated Rules for AutoKey IKE RAS VPN
10. Add the VPN Link. You must create a VPN link between the Security Policy and the VPN Manager autogenerated rules. You create this link by inserting a VPN link in the Security Policy; this links points to the VPN rules that exist in the VPN Manager.


   b. Select the UNIX Remote Access VPN.

   c. Click OK to add the link to the policy. By default, the link appears at the top of the policy, but you can move the VPN link anywhere in the policy, just as you would a firewall rule.

EXAMPLE: CONFIGURING AN AUTOKEY IKE, ROUTE-BASED SITE-TO-SITE VPN
In this example, an AutoKey IKE VPN tunnel using a preshared key provides a secure connection between security devices protecting the Tokyo and Paris offices. The Untrust zone interface for both security devices use a static IP address. All security and tunnel zones are in the trust-vr. The preshared key is h1p8A24nG5. For the Phase 1 and 2 security levels, specify the Phase 1 proposal as pre-g2-3des-sha and the Phase 2 proposal as predefined compatible.

Figure 158: AutoKey IKE, RB Site-to Site VPN Example Overview

1. Add the Tokyo and Paris security devices (for details on adding devices, see Chapter 4, “Adding Devices”):

   a. Configure the Tokyo device with the following interfaces:
      - Ethernet1 is the Trust IP (10.1.1.1/24) in the Trust zone.
      - Ethernet3 is the Untrust IP (1.1.1.1/24).

   b. Configure the Paris device with the following interfaces:
      - Ethernet1 is the Trust IP (10.2.2.1/24) in the Trust zone.
Ethernet3 is the Untrust IP (2.2.2.2/24) in the Untrust zone.

2. Create the Address Objects that you use for the VPN rule in the firewall rulebase (for details on creating VPN rules, see “Adding VPN Rules” on page 664).
   a. Add the Tokyo Trust LAN (10.1.1.0/24) as a network Address Object. In Address Objects, click the Add icon and select Network. Configure the following, then click OK:
      - For Name, enter Tokyo Trust LAN
      - For IP Address/Netmask, enter 10.1.1.0/24
      - For Color, select magenta.
      - For Comment, enter Tokyo Trust Zone.
   b. Add the Paris Trust LAN (10.2.2.0/24) as a network Address Object. In Address Objects, click the Add icon and select Network. Configure the following, then click OK:
      - For Name, enter Paris Trust LAN
      - For IP Address/Netmask, enter 10.2.2.0/24
      - For Color, select magenta.
      - For Comment, enter Paris Trust Zone.

3. Create the VPN. In the navigation tree, double-click VPN Manager, right-click VPNs and select AutoKey IKE VPN. The New AutoKey IKE VPN dialog box appears. Configure as shown below:
   a. In Name, enter Tokyo-Paris Route-Based VPN.
   b. Select Enable.
   c. In Termination Point, select Untrust.
   d. Click OK to save the VPN and return to VPN Manager. In VPN Manager, select the Tokyo-Paris Route-Based VPN.

4. Configure the route-based members:
   a. In the main display area, select the security device link (under Route-Based Configuration) to display the zone and tunnel options. Configure the default zone and tunnel options as shown below:
b. Click the Add icon to display available security devices. Select the Paris and Tokyo devices.

c. Click OK to add the members to the VPN.

d. Ensure that the route-based members are configured as shown below:

![Select Devices]

<table>
<thead>
<tr>
<th>Firewall Device</th>
<th>Tunnel Interface Zone</th>
<th>Physical Source Interface</th>
<th>Single Tunnel Interface</th>
<th>NHTB entries</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paris</td>
<td>untrust</td>
<td>ethernet3</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Tokyo</td>
<td>untrust</td>
<td>ethernet3</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

e. Click OK to save your settings and return to the main display area.

5. Configure the VPN topology:

a. Select the Topology link. The Topology dialog box appears.

b. Click the Add icon to display the Topology configuration dialog box.

![View Members for AutoKey IKE, RB Site-to Site VPN]

![Select Devices]

<table>
<thead>
<tr>
<th>Firewall Device</th>
<th>Tunnel Interface Zone</th>
<th>Physical Source Interface</th>
<th>Single Tunnel Interface</th>
<th>NHTB entries</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paris</td>
<td>untrust</td>
<td>ethernet3</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Tokyo</td>
<td>untrust</td>
<td>ethernet3</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

c. In the Mains window, select the Paris and Tokyo security devices.

d. Click OK to return to the Topology dialog box, then click OK to return to the main display area.

6. Configure the termination points of the VPN:

a. Click the Termination Points link. The Termination Points dialog box appears.

b. Confirm that both Paris and Tokyo devices use a Termination Interface of ethernet3, then click OK to return to the main display area.

7. Configure the VPN gateway:

a. Click the Gateway Parameters link. The Properties tab appears. Leave all defaults and click the Security tab.
b. In the Security tab, enter the preshared key value (h1p8A24nG5), then click Generate Key.

c. For Phase 1 Proposals, select User-Defined, then click the Add/Edit icon to add the pre-g2-3des-sha proposal, as shown below:

Figure 161: Configure Security for AutoKey IKE, RB Site-to Site VPN

8. Click Save to save your configuration changes to the VPN. Because this VPN is route-based, no rules are autogenerated. However, you can view the device tunnel summary to see all autogenerated tunnels between each security device in the VPN, as shown below:

Figure 162: View Tunnel Summary for AutoKey IKE, RB Site-to Site VPN

A tunnel interface acts as a doorway to a VPN tunnel; traffic enters and exits a VPN tunnel via a tunnel interface. These tunnels are an “always-on” connection—the devices will route any traffic with an appropriate source and destination IP address through the VPN tunnel.

To control traffic through the tunnel, you must add firewall rules to the Security Policy that is installed on each VPN node. For details on creating firewall rules, see “Configuring Firewall Rules” on page 536.
Next, you must create the routes (in the route table of each device) that will connect the autogenerated tunnel interfaces and form the VPN tunnel (for details on creating routes, see “Configuring Virtual Routers” on page 169). You can use static or dynamic routes, however, this example details only the static route creation. For each device, you will create two routes using the trust virtual router (trust-vr):

- A route from 0.0.0.0/0 to eth3 in the untrust zone. This routes traffic from the trust zone through eth3 in the untrust zone, then to the next hop (default) gateway.

- A route from the tunnel.1 interface (autogenerated by VPN Manager) to the untrust zone of the remote VPN node. This routes traffic destined for the remote VPN node through the tunnel.1 interface (where the packets are encapsulated), with a default next hop gateway of 0.0.0.0/0.

9. Configure the route on the Tokyo security device.

   a. In Device Manager, double-click the device to open the device configuration dialog box. Select Network > Virtual Router to display the list of virtual routers on the device.

   b. Double-click the trust-vr route to open the vr for editing. In the virtual router dialog box, click Routing Table, then click the add icon under destination-based Routing Table to add a new static route.

   c. Configure a route from the untrust interface to the gateway, as shown below:

   ![Figure 163: Configure Untrust Route for AutoKey IKE, RB Site-to Site VPN]

   NOTE: ScreenOS 4.0.x devices display only the destination-based Routing Table; ScreenOS 5.x devices display both destination-based and source-based routing tables.
d. Configure route from the trust zone to the tunnel interface, as shown below:

Figure 164: Configure Trust Route for AutoKey IKE, RB Site-to Site VPN

Your routing table should appear as shown below:

Figure 165: View Routing Table for AutoKey IKE, RB Site-to Site VPN

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Mask</th>
<th>Next Hop</th>
<th>Yesys</th>
</tr>
</thead>
</table>
| 0.0.0.0    | 0    | Interface: ethernet3  
|            |      | Gateway IP Address: 1.1.1.250  
|            |      | Metric: 1  
|            |      | Tag:       
| 10.2.2.0   | 24   | Interface: tunnel.1  
|            |      | Gateway IP Address: 0.0.0.0  
|            |      | Metric: 1  
|            |      | Tag:       |

e. Click OK to save your changes to the virtual router, then click OK to save your changes to the Tokyo device.

10. Configure the route on the Paris security device:

a. In Device Manager, double-click the device to open the device configuration dialog box. Select Network > Virtual Router to display the list of virtual routers on the device.
b. Double-click the trust-vr route to open the vr for editing. In the virtual router dialog box, click Routing Table, then click the add icon under destination-based Routing Table to add a new static route.

NOTE: ScreenOS 4.0.x devices display only the destination-based Routing Table; ScreenOS 5.x devices display both destination-based and source-based routing tables.

c. Configure a route from the untrust interface to the gateway, as shown below:

Figure 166: Configure Untrust Route for AutoKey IKE, RB Site-to Site VPN

![New Routing Table](image)

IP Address: 0.0.0.0
Network Mask: 
Next Hop: Gateway
Interface: ethernet3
Gateway IP Address: 2.2.2.250
Metric: 1
Tag: none

![OK and Cancel buttons]

d. Configure route from the trust zone to the tunnel interface, as shown below:

Figure 167: Configure Trust Route for AutoKey IKE, RB Site-to Site VPN

![New Routing Table](image)

IP Address: 10.1.1.0
Network Mask: 24
Next Hop: Gateway
Interface: tunnel.1
Gateway IP Address: 0.0.0.0
Metric: 1
Tag: none

![OK and Cancel buttons]
Your routing table should appear as shown below:

**Figure 168: View Routing Table for AutoKey IKE, RB Site-to Site VPN**

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Mask</th>
<th>Next Hop</th>
<th>Vsys</th>
</tr>
</thead>
</table>
| 0.0.0.0    | 0    | Interface: ethernet3  
|           |      | Gateway IP Address: 2.2.2.250  
|           |      | Metric: 1  
|           |      | Tag: | ... |
| 10.1.1.0   | 24   | Interface: tunnel 1  
|           |      | Gateway IP Address: 0.0.0.0  
|           |      | Metric: 1  
|           |      | Tag: | ... |

e. Click OK to save your changes to the virtual router, then click OK to save your changes to the Paris device.

**EXAMPLE: CONFIGURING XAUTH AUTHENTICATION WITH EXTERNAL USER GROUP**

In this example, you use a VPN to enable access for a group of resellers who require access to FTP servers in the corporate LAN. First, you must configure the RADIUS server using the custom port 4500 (default is 1645), then add an authentication server object in NetScreen-Security Manager to represent that server.

Next, to manage the users in this example, you define an external user group in two places: on the external RADIUS auth server and in NetScreen-Security Manager.

- On the RADIUS server, you populate the external user group with XAuth users, leaving the group unpopulated in NetScreen-Security Manager. The RADIUS server authenticates the users during Phase 1 IKE negotiations.

- In NetScreen-Security Manager, you leave the external user group unpopulated, but you must define each user as a local user with an IKE ID, then create a group that includes those local users as members. This IKE ID is used to authenticate the users during the Phase 2 IKE negotiations.

Additionally, you must add the security device and create an Address object to represent the FTP server, as well as a protected resource. After you have assembled all the VPN components, you are ready to create the VPN.

1. Configure the RADIUS Server. On the RADIUS server, load the Juniper Networks dictionary file and define Xauth user accounts. Use the Juniper Networks user group VSA to create the user group xa_grp2 and apply it to the auth user accounts that you want to add to that group.

**NOTE:** For instructions on loading the dictionary file onto a RADIUS server, refer to the RADIUS server documentation. If you are using a Microsoft IAS RADIUS server, there is no dictionary file to load. Instead, define the correct vendor-specific attributes (VSAs) on the server.
2. Configure the VPN Components:

a. Add the Authentication Server Object. In the main navigation tree, select Object Manager > Authentication Servers and click the Add icon. Configure the following, then click OK:

- For name, enter radius1. Select a color and add a comment, if desired.
- For Main Server, enter the IP 10.20.1.100; for Primary Backup Server, enter IP 10.20.1.110; for Secondary Backup Server, enter IP 10.20.1.120.
- For timeout, enter 30.
- Enable For XAuth Users.
- For Server Type, select RADIUS, then configure the RADIUS server:
  - For server port, select 4500 (default is 1645)
  - For secret, enter A56hYY97kl
  - For retry timeout, enter 4.

b. Add an External User Group (in NetScreen-Security Manager). In the Object Manager, select User Objects > External User Groups. Click the Add icon to display the New External User Group dialog box. Configure the following, then click OK:

- For Name, enter xa-grp2.
- For Color, select yellow.
- For Comment, enter Reseller Group RADIUS.
- Enable XAuth.

c. Add the Local User Object. In the Object Manager, select User Objects > Local Users. Click the Add icon and select User. The New Local User dialog box appears. Configure the following, then click OK.

- For Name, enter jhansen.
- For Color, select orange.
- For Comment, enter reseller group.
- Select Enable, then select IKE.
- For IKE settings, enable User FQDN and enter the email address jhansen@company.com.

d. Add a Local User Group. In the Object Manager, select User Objects > Local User Groups. Click the Add icon to display the New Local User Group dialog box. Configure the following, then click OK:
For Name, enter Reseller User Group.

For color, enter green.

For Comment, enter Reseller VPN XAuth RADIUS.

Add jhansen as a member.

e. Add a Network address object to represent the network used by Reseller group. In the Object Manager, select Address Objects, then click the Add icon and select Network. The New Network dialog box appears. Configure the following, then click OK:

- For Name, enter reseller1.
- For IP Address/Netmask, enter 10.2.2.0/24.
- For color, select cyan.
- For Comment, enter Reseller Group.

f. Add an Address Object to represent the FTP Server. In the Object Manager, select Address Objects, then click the Add icon and select Host. The New Host dialog box appears. Configure the following, then click OK:

- For Name, enter rsl-svr1.
- For Color, select green.
- For Comment, enter FTP Server.
- Select IP, then enter the IP Address 10.1.1.5.

g. Add a NetScreen-208 security device named “Bozeman”. This is the device protects the FTP server (for details on adding devices, see Chapter 4, “Adding Devices”). Configure the Bozeman device with the following interfaces:

- Ethernet1 is the Trust IP (10.1.1.1/24) in the Trust zone.
- Ethernet3 is the Untrust IP (2.2.2.2/24) in the Untrust zone.

h. Create a Protected Resource to represent the destination point of the VPN (for details on creating Protected Resources, see “Configuring Protected Resources” on page 520). In this example, the destination point is the FTP server in the trust zone of Bozeman. In Protected Resources (under VPN Manager), click the Add icon. Configure the object as shown below, then click OK:
3. Create the VPN. In the main navigation tree, select VPN Manager > VPNs. Click the Add icon and select AutoKey IKE RAS VPN. The New AutoKey IKE RAS VPN dialog box appears. Configure as shown below:

   a. In Name, enter Reseller Remote Access VPN.
   
   b. Select Enable.
   
   c. In Termination Point, select Untrust.
   
   d. Click OK to save the VPN and return to VPN Manager. The Reseller Remote Access VPN appears in the main display area.

4. Configure the policy-based members:

   a. In the main display area, select the Protected Resources link.
   
   b. In the Protected Resources list, select the rsl-svr1 protected resource, then click OK:

5. Configure the termination points of the VPN:

   a. Click the Termination Points link. The Termination Points dialog box appears.
   
   b. Configure the Bozeman device to use ethernet3 as the termination point (this is the Untrust zone interface).
c. Click OK to return to the main display area.

6. Configure the remote users for the VPN:
   a. In the Remote Users section, click the Users link. The Remote User dialog box appears.
   b. Select the Reseller local user group as shown below:

   Figure 170: Configure Remote User (Reseller Local User Group)

   Remote User
   Users
   Reseller User Group

   c. Click Save to save your configuration changes to the VPN.

7. Configure the VPN gateway:
   a. Click the Gateway Parameters link. The Properties tab appears.
   b. For Mode, select Main.
   c. In the XAuth section, select XAuth Server and then select the radius1 authentication server for Auth Server Name. Later, after you have autogenerated the VPN rules and gateway, you can override this setting to include only the Reseller external user group. For details, see “Configure Overrides. By default, the gateway attempts to authenticate all users using the specified authentication server (radius1). You must override the gateway security settings to enable the VPN to authenticate only the Reseller external user group:” on page 649.
   d. In the Security tab, enter the preshared key value (netscreen4), then click Generate Key.
   e. For Phase 1 Proposals, select User-Defined, then click the Add/Edit icon to add the pre-g2-3des-sha proposal, as shown below:
Figure 171: Configure Security for Reseller VPN

<table>
<thead>
<tr>
<th>Properties</th>
<th>Security</th>
<th>IKE IDs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preshare Key/RSA/D5A</td>
<td><img src="image" alt="Preshare Key Information" /></td>
<td></td>
</tr>
<tr>
<td>Generate Key</td>
<td><img src="image" alt="Generate Key" /></td>
<td></td>
</tr>
<tr>
<td>Preshared Key</td>
<td><img src="image" alt="Preshared Key" /></td>
<td></td>
</tr>
</tbody>
</table>

Phase 1 Proposals

Security Level: ![User-Defined](image)

- pre-g2-3des-sha

f. Click Ok to save your changes to the gateway.

8. Click Save to save your configuration changes to the VPN and autogenerate the policy rules.

To view the autogenerated rules, click the Policy Rules link in the Overrides section. VPN Manager generates the rules as shown below:

Figure 172: View Autogenerated Rules for Reseller VPN

9. Configure Overrides. By default, the gateway attempts to authenticate all users using the specified authentication server (radius1). You must override the gateway security settings to enable the VPN to authenticate only the Reseller external user group:

a. In the overrides area, click the Device Configuration link.

b. In the navigation tree, double-click Bozeman and select Gateway. The autogenerated gateway for the Bozeman appears in the main display area.

c. Right-click the autogenerated gateway and select Edit. The Properties tab appears.

d. In the IKE IDs/XAuth tab, configure the XAuth area to authenticate only the Reseller external group, as shown below:
Figure 173: Configure IKE IDs/ XAuth Overrides for Reseller VPN

<table>
<thead>
<tr>
<th>XAuth Server</th>
<th>XAuth Server Name</th>
<th>Query Remote Type</th>
<th>User Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>radi1</td>
<td>Generic</td>
<td>User Group</td>
<td>xa-grp2</td>
</tr>
</tbody>
</table>

- For user, select User Group.
- For User Group, select xa-grp2.
- Click OK to save your overrides.

10. Add the VPN Link. You can create a VPN link between the Security Policy and the VPN Manager autogenerated rules. You create this link by inserting a VPN link in the Security Policy; this links points to the VPN rules that exist in the VPN Manager.


b. Select the Reseller Remote Access VPN.

c. Click OK to add the link to the policy.

By default, the link appears at the top of the policy, but you can move the VPN link anywhere in the policy, just as you would a firewall rule.

Creating Device-Level VPNs

You can create four types of device-level VPNs:

- Use an **AutoKey IKE VPN** to connect devices and/or protected resources. An AutoKey IKE VPN supports mixed-mode, policy-based, and routing-based VPNs, but does not support RAS users. For details on each step, see “Creating AutoKey IKE VPNs” on page 651.

- Use a **Manual Key IKE VPNs** to authenticate devices, protected resources, and RAS users in the VPN with manual keys. For details on each step, see “Creating Manual Key VPNs” on page 658.

- Use an **L2TP RAS VPN** to connect L2TP RAS users and protected resources with authentication but without encryption. For details on each step, see “Creating L2TP VPNs” on page 662.
Use an **L2TP-over-AutoKey IKE RAS VPN** to connect L2TP RAS users and protected resources. An L2TP-over-AutoKey IKE RAS VPN supports policy-based VPNs and L2TP RAS users, but does not support routing-based VPNs. For details on each step, see “Creating L2TP Over Autokey IKE VPNs” on page 663.

**Supported Configurations**

IKE VPNs support tunnel mode, and can be policy-based or route-based; however, route-based VPNs do not support RAS users.

L2TP VPNs support transport mode, and can be policy-based.

**Creating AutoKey IKE VPNs**

Creating device-level AutoKey IKE VPNs is a four stage process:

- Configure Gateway
- Configure Routes (Route-based only)
- Configure VPN on the Device
- Add VPN rules to Security Policy

**Configuring Gateways**

A gateway is an interface on your security device that sends and receives traffic; a remote gateway is an interface on another device that handles traffic for that device. Each security device member has a remote gateway that it sends and receives VPN traffic to and from. To configure a gateway for a VPN member, you need to define the local gateway (the interface on the VPN member that handles VPN traffic) and the remote gateway (the interface on the other VPN member that handles VPN traffic). The interface can be physical or virtual.

- For remote gateways that use static IP addresses, specify the IP address or host name of the remote device.
- For remote gateways that use dynamic IP addresses, configure an IKE ID for the remote device.
- For remote gateways that are RAS users, specify a Local User object as a remote gateway to enable RAS user access.

To add a gateway to a security device, open the device configuration, select VPN Settings, and click the Add icon to display the New Gateway Dialog box. Configure the gateway as detailed in the following sections.

**Properties**

Enter a name for the new gateway, then specify the following gateway values:

- Mode—The mode determines how Phase 1 negotiations occur.
In Main mode, the IKE identity of each node is protected. Each node sends three two-way messages (six messages total); the first two messages negotiate encryption and authentication algorithms that protect subsequent messages, including the IKE identity exchange between the nodes. Depending on the speed of your network connection and the encryption and authentication algorithms you use, main mode negotiations can take a long time to complete. Use Main mode when security is more important.

In Aggressive mode, the IKE identity of each node is not protected. The initiating node sends two messages and the receiving node sends one (three messages total); all messages are sent in the clear, including the IKE identity exchange between the nodes. Because Aggressive mode is typically faster but less secure than Main mode, use Aggressive mode when speed is more important than security. However, you must use Aggressive mode for VPNs that include RAS users.

Remote Gateway—The remote gateway is the VPN gateway on the receiving VPN node, and can be an interface with a static or dynamic IP address, or local or external user object.

Static IP Address. For remote gateways that use a static IP address, enter the IP address and mask.

RAS User/Group. For remote gateways that are users, select the User object or User Group object that represents the RAS user.

Dynamic IP Address. For remote gateways that use a dynamic IP address, select dynamic IP address.

Outgoing Interface—The outgoing interface (also known as the termination interface) is the interface on the security device that sends and receives VPN traffic. Typically, the outgoing interface is in the untrust zone.

Heartbeats—Use heartbeats to enable redundant gateways. You can use the default or set your own thresholds:

Hello. Enter the number of seconds the security device waits between sending hello pulses.

Reconnect. Enter the maximum number of seconds the security device waits for a reply to the hello pulse.

Threshold. Enter the number of seconds that the security device waits before attempting to reconnect.

NAT Traversal—Because NAT obscures the IP address in some IPSec packet headers, a VPN node cannot receive VPN traffic that passes through an external NAT device. To enable VPN traffic to traverse a NAT device, you can use NAT Traversal (NAT-T) to encapsulate the VPN packets in UDP. If a VPN node with NAT-T enabled detects an external NAT device, it checks every VPN packet to determine if NAT-T is necessary. Because checking every packet impacts VPN performance, you should only use NAT Traversal for remote users that must connect to the VPN over an external NAT device.
Creating Device-Level VPNs

Chapter 10: Configuring VPNs

You do not need to enable NAT-T for your internal security device nodes that use NAT; each VPN node knows the correct address translations for VPN traffic and does not need to encapsulate the traffic.

To use NAT-T, enable NAT-Traversal and specify:

- **UDP Checksum.** A 2-byte value (calculated from the UDP header, footer, and other UDP message fields) that verifies packet integrity. You must enable this option for NAT devices that require UDP checksum verification; however, most NAT devices (including security devices) do not require it.

- **Keep alive Frequency.** The number of seconds a VPN node waits between sending empty UDP packets through the NAT device. A NAT device keeps translated IP addresses active only during traffic flow, and invalidates unused IP addresses. To ensure that the VPN tunnel remains open, you can configure the VPN node to send empty “keep alive” packets through the NAT device.

**IKE IDs/XAuth**

Every VPN member has a unique identification number, known as an IKE ID. During Phase 1 negotiations, the IKE protocol uses the ID to authenticate the VPN member. You must select and configure an ID type for the VPN members at each end of the tunnel. However, the ID type can be different for each member:

- **ASN1-DN—**Abstract Syntax Notation, version 1 is a data representation format that is non-platform specific; Distinguished Name is the name of the computer. Use ASN1-DN to create a Group ID that enables multiple RAS users to connect to the VPN tunnel concurrently.

  - At the peer ID, specify values for the Container Match and Wildcard Match.

  - At the local ID, specify the value.

Using a Group ID can make configuring and maintaining your VPN quicker and easier. For details on how Group IKE IDs work, see “Configuring Group IKE IDS” on page 607. For details on determining the ASN1-DN container and wildcard values for Group IKE IDs, see Juniper Networks ScreenOS 5.x Concepts and Examples Guide.

- **FQDN—**Use a Fully Qualified Domain Name when the VPN member uses a dynamic IP address. FQDN is a name that identifies (qualifies) a computer to the DNS protocol using the computer name and the domain name; ex. server1.colorado.mycompany.com.

- **IP Address—**Use an IP address when the VPN member uses a static IP address.

- **U-FQDN—**Use a User Fully Qualified Domain Name when the VPN member uses a dynamic IP address (such as a RAS user). A U-FQDN is a simply an email address; ex. user1@mycompany.com.

Use the XAuth protocol to authenticate RAS users with an authentication token (such as SecureID) and to make TCP/IP settings (IP address, DNS server, and WINS server) for the peer gateway.
Default Server—Use the default server to use the default XAuthentication server for the device. To change or assign a default XAuthentication server, edit the VPN settings > Defaults > Xauth settings.

XAuth Server—Use to specify the authentication server that assigns TCP/IP settings to the remote gateway.

- XAuth Server Name. Select a pre-configured authentication server object. For details on creating authentication server objects, see “Configuring Authentication Servers” on page 498.
- Allowed Authentication Type. Select generic or Challenge Handshake Authentication Protocol (CHAP) (password is sent in the clear) to authenticate the remote gateway.
- Query Remote Setting. Enable this option to query the remote settings object for DNS and WINS information.
- Users and Groups. To authenticate XAuth RAS users using the authentication server, enable User or User Group and select a preconfigured user object.

XAuth Client—Use when the remote gateway is a RAS user that you want to authenticate.

- Allowed Authentication Type. Select Any or Challenge Handshake Authentication Protocol (CHAP) for authentication (password is sent in the clear).
- User Name and Password. Enter the user name and password that the RAS user must provide for authentication.

NOTE: All passwords handled by NetScreen-Security Manager are case-sensitive.

Bypass Authentication—Use to permit VPN traffic from this VPN member to pass unauthenticated by the Auth server.

Security
Select the authentication method you want to use in the VPN:

- Preshared Key—Use if your VPN includes security devices and/or RAS users. VPN nodes use the preshared key during Phase 1 negotiations to authenticate each other; because each node knows the key in advance, negotiations use fewer messages and are quicker.
To generate a random key, enter a value for the seed, then click Generate Key. NetScreen-Security Manager uses the seed value to generate a random key, which is used to authenticate VPN members.

NOTE: Using a random key can generate a value in excess of 255 characters, which exceeds ScreenOS limits and might not be accepted by the security device during update. To reduce the key size, shorten the autogenerated key value by deleting characters.

To use a predefined value for the key, enter a value for the Preshared Key.

PKI—Use if your VPN includes extranet devices or you require the additional security provided by certificates (PKI uses certificates for VPN member authentication). For details on creating and managing certificates, see “Configuring Certificate Authorities” on page 517.

For Phase 1 negotiations, select a proposal or proposal set. You can select from predefined or user-defined proposals:

- To use a predefined proposal set, select one of the following:
  - Basic (nopfs-esp-des-sha, nopfs-esp-des-md5)
  - Compatible (nopfs-esp-3des-sha, nopfs-esp-3des-md5, nopfs-esp-des-sha, nopfs-esp-des-md5)
  - Standard (gs-esp-3des-sha, gs-esp-aes128-sha)

NOTE: You cannot use a predefined proposal set with certificates—you must select a user-defined proposal or change the authentication method to Preshared Key.

To use a user-defined proposal, select a single proposal from the list of predefined and custom IKE Phase 1 Proposals. For details on custom IKE proposals, see “Configuring IKE Proposals” on page 523.

If your VPN includes only security devices, you can specify one predefined or custom proposal that NetScreen-Security Manager propagates to all nodes in the VPN. If your VPN includes extranet devices, you should use multiple proposals to increase security and ensure compatibility.

Configuring Routes (Route-based only)

For a routing-based VPN member, you must configure:

- Tunnel zone or tunnel interfaces on the member.
- Static or dynamic routes from the member to other VPN members.

VPN traffic flows through the tunnel zones or tunnel interfaces on the security device, and uses static or dynamic routes to reach other VPN members. You must create the tunnel zones and interfaces before configuring routes.
For details on configuring tunnel zones, tunnel interfaces, static routes, or dynamic routes, see “Configuring Virtual Routers” on page 169.

After you have configured the tunnel zone or interface on the security device, you must bind the VPN to that zone or interface to make the VPN functional, as described in the following section.

Configuring the VPN

When you configure the VPN, you are defining the gateway the security device uses to connect to the VPN, the IKE Phase 2 proposals used by that gateway, and how you want NetScreen-Security Manager to monitor the VPN tunnel.

For route-based VPNs, you are also binding the VPN to the tunnel interface or zone that sends and receives VPN traffic to and from the device.

Properties

Enter the following values:

- **VPN name**—Enter a name for the VPN.
- **Remote Gateway**—Select the gateway for the VPN.
- **Idle Time to Disable SA**—Configure the number of minutes before a session that has no traffic automatically disables the SA.
- **Replay Protection**—In a replay attack, an attacker intercepts a series of legitimate packets and uses them to create a denial-of-service (DoS) against the packet destination or to gain entry to trusted networks. If replay protection is enabled, your security devices inspect every IPSec packet to see if the packet has been received before—if packets arrive outside a specified sequence range, the security device rejects them.
- **IPSec Mode**—Configure the mode:
  - Use tunnel mode for IPSec. Before an IP packet enters the VPN tunnel, NetScreen-Security Manager encapsulates the packet in the payload of another IP packet and attaches a new IP header. This new IP packet can be authenticated, encrypted, or both.
  - Use transport mode for L2TP-over-IPSec. NetScreen-Security Manager does not encapsulate the IP packet, meaning that the original IP header must remain in plaintext. However, the original IP packet can be authenticated, and the payload can be encrypted.
  - Do not set Fragment Bit in the Outer Header—The Fragment Bit controls how the IP packet is fragmented when traveling across networks.
    - Clear. Use this option to enable IP packets to be fragmented.
    - Set. Use this option to ensure that IP packets are not fragmented.
    - Copy. Select to use the same option as specified in the internal IP header of the original packet.
Security

For Phase 2 negotiations, select a proposal or proposal set. You can select from predefined or user-defined proposals:

- To use a predefined proposal set, select one of the following:
  - Basic (nopfs-esp-des-sha, nopfs-esp-des-md5)
  - Compatible (nopfs-esp-3des-sha, nopfs-esp-3des-md5, nopfs-esp-des-sha, nopfs-esp-des-md5)
  - Standard (gs-esp-3des-sha, gs-esp-aes128-sha)

- To use a user-defined proposal, select a single proposal from the list of predefined and custom IKE Phase 2 Proposals. For details on custom IKE proposals, see “Configuring IKE Proposals” on page 523.

If your VPN includes only security devices, you can specify one predefined or custom proposal that NetScreen-Security Manager propagates to all nodes in the VPN. If your VPN includes extranet devices, you should use multiple proposals to increase security and ensure compatibility.

Binding/ProxyID

You can bind the VPN tunnel to a tunnel interface or tunnel zone to increase the number of available interfaces in the security device. To use a tunnel interface and/or tunnel zone in your VPN, you must first create the tunnel interface or zone on the device; for details, see “Configuring Tunnel Interfaces and Tunnel Zones” on page 608 and “Configuring a Tunnel Interface” on page 258.

- None—Select none when you do not want to bind the VPN tunnel to a tunnel interface or zone.
- Tunnel Interface—Select a pre-configured tunnel interface on the security device to bind the VPN tunnel to the tunnel interface. The security device routes all VPN traffic through the tunnel interface to the protected resources.
- Tunnel Zone—Select a pre-configured tunnel zone on the security device to bind the VPN tunnel directly to the tunnel zone. The tunnel zone must include one or more numbered tunnel interfaces; when the security device routes VPN traffic to the tunnel zone, the traffic uses one or more of the tunnel interfaces to reach the protected resources.

You can also enable proxy and configure the proxy parameters.

Monitor

You can enable VPN Monitor and configure the monitoring parameters for the device. Monitoring is off by default. To enable the VPN Monitor in Realtime Monitor to display statistics for the VPN tunnel, configure the following:
VPN Monitor—When enabled, the device sends ICMP echo requests (pings) through the tunnel at specified intervals (configurable in seconds) to monitor network connectivity (the device uses the IP address of the local outgoing interface as the source address and the IP address of the remote gateway as the destination address). If the ping activity indicates that the VPN monitoring status has changed, the device triggers an SNMP trap; VPN Monitor (in RealTime Monitor) tracks these SNMP statistics for VPN traffic in the tunnel and displays the tunnel status.

Rekey—When enabled, the device regenerates the IKE key after a failed VPN tunnel attempts to re-establish itself. When disabled, the device monitors the tunnel only when the VPN passes user-generated traffic (instead of using device-generated ICMP echo requests). Use the rekey option to:

- Keep the VPN tunnel up even when traffic is not passing through
- Monitor devices at the remote site.
- Enable dynamic routing protocols to learn routes at a remote site and transmit messages through the tunnel.
- Automatically populate the next-hop tunnel binding table (NHTB table) and the route table when multiple VPN tunnels are bound to a single tunnel interface.

Optimized—(This option appears only for devices running ScreenOS 5.x.) When enabled, the device optimizes its VPN monitoring behavior as follows:

- Considers incoming traffic in the VPN tunnel as ICMP echo replies. This reduces false alarms that might occur when traffic through the tunnel is heavy and the echo replies cannot get through.
- Suppresses VPN monitoring pings when the tunnel passes both incoming and outgoing traffic. This can help reduce network traffic.

Source Interface and Destination IP—Configure these options to use VPN Monitoring when the other end of the VPN tunnel is not a security device. Specify the source and destination IP addresses.

Adding a VPN Rule
After you have configured the VPN on each device you want to include in the VPN, you can add a VPN rule to a Security Policy:

- For policy-based VPNs, you must add a VPN rule to create the VPN tunnel.
- For route-based VPNs, the VPN tunnel is already in place. However, you might want to add a VPN rule to control traffic through the tunnel.

For details on adding and configuring a VPN rule in a Security Policy, see “Adding VPN Rules” on page 664.

Creating Manual Key VPNs
Creating a device-level Manual Key VPN is a four stage process:
1. Configure XAuth Users
2. Configure Routes (Route-based only)
3. Configure VPN on Device
4. Add VPN rules to Security Policy

Adding XAuth Users
For VPNs that use IPSec manual key to provide remote access services, you must add an XAuth User to the security device. An XAuth User has an account on the security device that guards the protected resources in the VPN; when the user attempts to connect to a protected resource, the security device authenticates the user.

To add a XAuth User for a security device, in the security device configuration L2TP/XAuth/Local User, click the Add icon. Enter a name for the user, then specify:

- **User**—Select a preconfigured Local User object that is configured for XAuth.
- **Remote Setting**—Select a preconfigured Remote Settings object.
- **IP Pool**—Select a preconfigured IP Pool object.
- **Static IP**—Enter the static IP address of the Local User.

Configuring Routes (Route-based only)
For a routing-based VPN member, you must configure:

- **Tunnel zone or tunnel interfaces on the member.**
- **Static or dynamic routes from the member to other VPN members.**

VPN traffic flows through the tunnel zones or tunnel interfaces on the security device, and uses static or dynamic routes to reach other VPN members. You must create the tunnel zones and interfaces before configuring routes. For details on configuring tunnel zones, tunnel interfaces, and static or dynamic routes, see “Configuring Virtual Routers” on page 169.

After you have configured the tunnel zone or interface on the security device, you must bind the VPN to that zone or interface to make the VPN functional, as described in the following section.

Configuring the VPN
The following sections detail how to configure the VPN.

**Properties**
Enter the following values:

- **VPN name**—Enter a name for the VPN.
Creating Device-Level VPNs

- **Gateway**—Enter a gateway for the VPN.

- **Local SPI**—The local Security Parameter Index.

- **Remote SPI**—The remote Security Parameter Index.

- **Outgoing Interface**—The outgoing interface is the interface on the security device that sends and receives VPN traffic. Typically, the outgoing interface is in the untrust zone.

- **Do not set Fragment Bit in the Outer Header**—The Fragment Bit controls how the IP packet is fragmented when traveling across networks.
  - **Clear**. Use this option to enable IP packets to be fragmented.
  - **Set**. Use this option to ensure that IP packets are not fragmented.
  - **Copy**. Select to use the same option as specified in the internal IP header of the original packet.

- **IPSec Protocol**—Specify the IPSec protocol and algorithm you want to use for data authentication and/or encryption. Because this information is static for each VPN member, they do not need to negotiate for communication.
  - **AH**. Use Authentication Header to authenticate the VPN traffic, but not encrypt the traffic. If you select AH, you must also specify the key or password that AH uses in the authentication algorithm.
  - **ESP**. Use Encapsulating Security Payload to authenticate and encrypt the VPN traffic. If you select ESP, because ESP uses keys to encrypt and decrypt data, you must also specify the key or password that the VPN node uses to send and receive VPN data through the VPN tunnel.

**NOTE:** All passwords handled by NetScreen-Security Manager are case-sensitive.

- **Binding**
  You can bind the VPN tunnel to a tunnel interface or tunnel zone to increase the number of available interfaces in the security device. To use a tunnel interface and/or tunnel zone in your VPN, you must first create the tunnel interface or zone on the device; for details, see “Configuring Tunnel Interfaces and Tunnel Zones” and “Configuring a Tunnel Interface” on page 258.

  - **None**—Select none when you do not want to bind the VPN tunnel to a tunnel interface or zone.

  - **Tunnel Interface**—Select a pre-configured tunnel interface on the security device to bind the VPN tunnel to the tunnel interface. The security device routes all VPN traffic through the tunnel interface to the protected resources.
Tunnel Zone—Select a pre-configured tunnel zone on the security device to bind the VPN tunnel directly to the tunnel zone. The tunnel zone must include one or more numbered tunnel interfaces; when the security device routes VPN traffic to the tunnel zone, the traffic uses one or more of the tunnel interfaces to reach the protected resources.

Monitor
You can enable VPN Monitor and configure the monitoring parameters for the device. Monitoring is off by default. To enable the VPN Monitor in Realtime Monitor to display statistics for the VPN tunnel, configure the following:

- **VPN Monitor**—When enabled, the device sends ICMP echo requests (pings) through the tunnel at specified intervals (configurable in seconds) to monitor network connectivity (the device uses the IP address of the local outgoing interface as the source address and the IP address of the remote gateway as the destination address). If the ping activity indicates that the VPN monitoring status has changed, the device triggers an SNMP trap; VPN Monitor (in RealTime Monitor) tracks these SNMP statistics for VPN traffic in the tunnel and displays the tunnel status.

- **Rekey**—When enabled, the device regenerates the IKE key after a failed VPN tunnel attempts to re-establish itself. When disabled, the device monitors the tunnel only when the VPN passes user-generated traffic (instead of using device-generated ICMP echo requests). Use the rekey option to:
  - Keep the VPN tunnel up even when traffic is not passing through.
  - Monitor devices at the remote site.
  - Enable dynamic routing protocols to learn routes at a remote site and transmit messages through the tunnel.
  - Automatically populate the next-hop tunnel binding table (NHTB table) and the route table when multiple VPN tunnels are bound to a single tunnel interface.

- **Optimized**—(This option appears only for devices running ScreenOS 5.x.) When enabled, the device optimizes its VPN monitoring behavior as follows:
  - Considers incoming traffic in the VPN tunnel as ICMP echo replies. This reduces false alarms that might occur when traffic through the tunnel is heavy and the echo replies cannot get through.
  - Suppresses VPN monitoring pings when the tunnel passes both incoming and outgoing traffic. This can help reduce network traffic.

- **Source Interface and Destination IP**—Configure these options to use VPN Monitoring when the other end of the VPN tunnel is not a security device. Specify the source and destination IP addresses.

Adding a VPN Rule
After you have configured the VPN on each device you want to include in the VPN, you can add a VPN rule to a Security Policy:
Creating Device-Level VPNs

For policy-based VPNs, you must add a VPN rule to create the VPN tunnel.

For route-based VPNs, the VPN tunnel is already in place. However, you might want to add a VPN rule to control traffic through the tunnel.

For details on adding and configuring a VPN rule in a Security Policy, see “Adding VPN Rules” on page 664.

Creating L2TP VPNs

Creating device-level L2TP VPN is a three stage process:

1. Add L2TP Users
2. Configure L2TP Settings
3. Add VPN rules to Security Policy

Adding L2TP Users

For VPNs that use L2TP to provide remote access services, you must add an L2TP User to the security device. An L2TP User has an account on the security device that guards the protected resources in the VPN; when the user attempts to connect to a protected resource, the security device authenticates the user.

To add a L2TP User for a security device, in the security device configuration L2TP/XAuth/Local User, click the Add icon. Enter a name for the user, then specify:

- **User**—Select a preconfigured Local User object that is configured for L2TP.
- **Remote Setting**—Select a preconfigured Remote Settings object.
- **IP Pool**—Select a preconfigured IP Pool object.
- **Static IP**—Enter the static IP address of the Local User.

Configuring L2TP

To connect to an L2TP VPN tunnel, the L2TP RAS user uses the IP address and WINS/DNS information assigned by the user’s ISP. However, when the L2TP RAS user sends VPN traffic through the tunnel, the security device assigns a new IP address and WINS/DNS information that enables the traffic to reach the destination network.

Enter a name for the L2TP VPN, then specify the following information:

- **Host Name**—Enter the name of the L2TP host.
- **Outgoing Interface**—The outgoing interface is the interface on the security device that sends and receives VPN traffic. Typically, the outgoing interface is in the untrust zone.
- **Keep Alive**—The number of seconds a VPN member waits between sending hello packets to an L2TP RAS user.
■ Peer IP—Enter the IP address of the L2TP peer.

■ Secret—Enter the shared secret that authenticates communication in the L2TP tunnel.

■ Remote Settings—Select the preconfigured remote settings object that represents the DNS and WINS servers assigned to L2TP RAS users after they have connected to the tunnel.

■ IP Pool Name—Select the preconfigured IP pool object that represents the available IP addresses that can be assigned to L2TP RAS users after they have connected to the tunnel.

■ Auth Server
  ■ Use the default settings to use the default authentication server for the domain. To change or assign a domain authentication server, edit the domain settings; for details, see “Creating Subdomains” on page 64.
  ■ Use custom settings to specify a preconfigured authentication server object to assign TCP/IP settings to the gateway and authenticate specific L2TP User or User Groups.

Adding a VPN Rule
After you have configured the VPN on each device you want to include in the VPN, you can add a VPN rule to a Security Policy:

■ For policy-based VPNs, you must add a VPN rule to create the VPN tunnel.

■ For route-based VPNs, the VPN tunnel is already in place. However, you might want to add a VPN rule to control traffic through the tunnel.

For details on adding VPN rules to a Security Policy, see “Adding VPN Rules” on page 664.

Creating L2TP Over Autokey IKE VPNs
Creating a device-level L2TP-over-Autokey IKE VPN is a multi-stage process:

1. Add L2TP Users (see “Adding L2TP Users” on page 662)
2. Configure L2TP Settings (see “Configuring L2TP” on page 662)
3. Configure Peer Gateway (see “Configuring Gateways” on page 651)
4. Configure Routes (Route-based only) (see “Configuring Routes (Route-based only)” on page 655)
5. Add VPN to Device (see “Configuring the VPN” on page 656)
6. Add VPN rules to Security Policy (see “Adding a VPN Rule” on page 663)
Adding VPN Rules

To create a policy-based VPN or to add access policies to a route-based VPN, you must add a VPN rule to a Security Policy for each device in the VPN.

Adding a VPN Rule is a three stage process:

1. Configuring the VPN rule
2. Configure Security Policy
3. Installing the Security Policy

Configuring the VPN

In Security Policies, select a predefined Security Policy (or create a new policy), and add a VPN rule. Right-click in the Source Address, Destination Address, Action, or Install On column and select Configure VPN to display the Configure VPN dialog box.

- Select the source security device that contains the termination interface for the VPN tunnel.
- Select a VPN Type:
  - For IKE VPNs, select the VPN that you configured on the device.
  - For L2TP VPNs, you must also select the L2TP tunnel that you configured on the device.
- Select the Protected Resources for the VPN:
  - If both VPN termination points are security devices, choose the protected resources that represent the network components you want to protect. You can also select a predefined Global MIP or VIP for the device.
  - If the source VPN termination point is a RAS user, select Source is Dialup and choose the Protected Resources behind the destination VPN termination point that represent the network components you want to protect on the remote network.
  - If the destination VPN termination point is a RAS user, select Destination is Dialup and choose the Protected Resources behind the source VPN termination point that represent the network components you want to protect on the local network.

Configuring the Security Policy

To configure the remaining columns for the VPN rule:

- From Zone—Select the zone on the source VPN member that contains the termination interface for the VPN tunnel.
- To Zone—Select the zone on the destination VPN member that contains the termination interface for the VPN tunnel.
Device-Level VPN Examples

This section provides examples of the two device-level VPN types:

- Configuring a Route-Based Site-to-Site VPN, Manual Key
- Configuring a Policy-Based Site-to-Site VPN, Manual Key
- Configuring a Policy-Based RAS VPN, L2TP

The following sections provide step-by-step instructions on creating each type of device-level VPN.

NOTE: For examples on creating other VPN types using VPN Manager, see “VPN Manager Examples” on page 627.

EXAMPLE: CONFIGURING A ROUTE-BASED SITE-TO-SITE VPN, MANUAL KEY

In this example, a Manual Key tunnel provides a secure communication channel between offices in Tokyo and Paris. The Trust zones at each site are in NAT mode. The Trust and Untrust security zones are in the trust-vr routing domain, and the Untrust zone interface (ethernet3) serves as the outgoing interface for the VPN tunnel.

To set up the tunnel, you must configure the security devices at both ends of the tunnel. First, you create the VPN components that you use to build the VPN, such as the security devices and the shared Address Objects. Next, you create the tunnel interfaces for each device and configure the VPN tunnel. You must also add the necessary static routes on each device to create the VPN tunnel. Finally, you create firewall rules in a Security Policy to control VPN traffic between the two sites.
1. Add the Tokyo and Paris security devices (for details on adding devices, see Chapter 4, “Adding Devices”):
   
   a. Configure the Tokyo device with the following interfaces:
      
      - Ethernet1 is the Trust IP (10.1.1.1/24) in the Trust zone.
      - Ethernet3 is the Untrust IP (1.1.1.1/24) in the Untrust zone.
   
   b. Configure the Paris device with the following interfaces:
      
      - Ethernet1 is the Trust IP (10.2.2.1/24) in the Trust zone.
      - Ethernet3 is the Untrust IP (2.2.2.2/24) in the Untrust zone.

2. Create the Address Objects that you use in the VPN rule in the firewall rulebase (for details on creating VPN rules, see “Adding VPN Rules” on page 664).
   
   a. Add the Tokyo Trust LAN (10.1.1.0/24) as an network Address Object. In Address Objects, click the Add icon and select Network. Configure the following, then click OK:
      
      - For Name, enter Tokyo Trust LAN.
      - For IP Address/Netmask, enter 10.1.1.0/24.
      - For Color, select magenta.
      - For Comment, enter Tokyo Trust Zone.

   b. Add the Paris Trust LAN (10.2.2.0/24) as a network Address Object. In Address Objects, click the Add icon and select Network. Configure the following, then click OK:
      
      - For Name, enter Paris Trust LAN.
For IP Address/Netmask, enter 10.2.2.0/24.

For Color, select magenta.

For Comment, enter Paris Trust Zone.

3. Configure the Tokyo tunnel interface:
   a. In the navigation tree, select Device Manager > Security Devices, then double-click the Tokyo device to open the device configuration.
   b. In the device navigation tree, select Network > Interface. Click the Add icon and select Tunnel Interface. The General Properties screen for tunnel.1 appears.
   c. Configure the following, then click OK:
      - For Zone, select untrust.
      - For IP Options, select Unnumbered.
      - For Source Interface, select ethernet3.

4. Create the Tokyo VPN:
   a. In the device navigation tree, select VPN Settings > AutoKey IKE/Manual VPN.
   b. Select the Manual tab, then click the Add icon. The Properties screen appears. Configure the Properties tab as shown below:
      - For Name, enter Tokyo_Paris.
      - For Gateway, enter 2.2.2.2.
      - For Local SPI, enter 3020.
      - For Remote SPI, enter 3030.
      - For Outgoing Interface, select ethernet3.
      - For ESP/AH, select ESP CBC.
      - For Encryption Algorithm, select 3DES-CBC.
      - Select Generate Key by Password, then enter the password asdlk24234.
      - For Authentication Algorithm, select SHA-1.
      - Select Generate Key by Password, then enter the password PNa5134a.
   c. Select the Binding tab. Enable Tunnel Interface, then select tunnel.1.
   d. Click OK to save the new VPN.
5. Create Tokyo Routes:

a. In the device navigation tree, select Network > Virtual Router to display the list of virtual routers on the device. Double-click the trust-vr route to open the vr for editing.

b. In the virtual router dialog box, click Routing Table, then click the add icon under destination-based Routing Table to add a new static route.

NOTE: ScreenOS 4.0.x devices display only the destination-based Routing Table; ScreenOS 5.0.x devices display both destination-based and source-based routing tables; ScreenOS 5.1 and higher devices display destination-based, source-based, and source interface-based routing tables.

c. Configure a route from the untrust interface to the gateway, as shown below, then click OK:

Figure 175: Configure Tokyo Route for RB Site-to-Site VPN, MK

![New Routing Table dialog box]

| IP Address | 0. 0. 0. 0 |
| Network Mask | 0 |
| Next Hop | Gateway |
| Interface | ethernet3 |
| Gateway IP Address | 1. 1. 1.250 |
| Metric | 1 |
| Tag | none |

OK Cancel

d. Configure route from the trust zone to the tunnel interface, as shown below, then click OK:
Device-Level VPN Examples

Figure 176: Configure Tokyo Trust Route for RB Site-to-Site VPN, MK

Your routing table should appear as shown below:

Figure 177: View Tokyo Routing Table for RB Site-to-Site VPN, MK

6. Configure the Paris Tunnel Interface:

a. In Device Manager, double-click the device icon for Paris to open the device configuration.

b. In the device navigation tree, select Network > Interface. Click the Add icon and select Tunnel Interface. The General Properties screen appears.

c. Configure the following, then click OK:

   ■ For Zone, select untrust.
For IP Options, select Unnumbered.
For Source Interface, select ethernet3.

7. Create the Paris VPN:
   a. In the device navigation tree, select VPN Settings > AutoKey IKE/Manual VPN.
   b. Select the Manual tab, then click the Add icon. The Properties screen appears.
   c. Configure the following:
      - For Name, enter Paris_Tokyo.
      - For Gateway, enter 2.2.2.2.
      - For Local SPI, enter 3020.
      - For Remote SPI, enter 3030.
      - For ESP/AH, select ESP CBC.
      - For Encryption Algorithm, select 3DES-CBC, then select Generate Key by Password and enter the password asdlk24234.
      - For Authentication Algorithm, select SHA-1, then select Generate Key by Password and enter the password PNas134a.
   d. Select the Binding tab. Enable Tunnel Interface, then select tunnel.1.
   e. Click OK to save the new VPN.

   a. In the device navigation tree, select Network > Virtual Router to display the list of virtual routers on the device.
   b. Double-click the trust-vr route to open the vr for editing.
   c. In the virtual router dialog box, click Routing Table, then click the add icon under destination-based Routing Table to add a new static route.
   d. Configure a route from the untrust interface to the gateway, as shown below, then click OK:

   NOTE: ScreenOS 4.0.x devices display only the destination-based Routing Table; ScreenOS 5.0.x devices display both destination-based and source-based routing tables; ScreenOS 5.1 and higher devices display destination-based, source-based, and source interface-based routing tables.
Figure 178: Configure Paris Untrust Route for RB Site-to-Site VPN, MK

Your routing table should appear as shown below:

![Routing Table](image)

e. Configure route from the trust zone to the tunnel interface, as shown below, then click OK:

Figure 179: Configure Paris Trust Route for RB Site-to-Site VPN, MK

Your routing table should appear as shown below:
9. Create the Security Policy:
   a. In the main navigation tree, select Security Policies. Click the Add icon to display the New Security Policy dialog box.
   b. Configure the following, then click OK:
      ■ For Security Policy Name, enter Corporate Route-Based VPN.
      ■ Add comments, if desired.
   c. In the main navigation tree, select Security Policies > Corporate Route-Based VPN. The security policy appears in the main display area. Configure the rules as shown below:

   Figure 181: Configure Rules for RB Site-to-Site VPN, MK

<table>
<thead>
<tr>
<th>No.</th>
<th>From Zone</th>
<th>Source</th>
<th>Match</th>
<th>To Zone</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>trust</td>
<td>Tokyo Trust LAN</td>
<td>untrust</td>
<td>trust</td>
<td>Paris Trust LAN</td>
<td>RNY any</td>
<td>permit</td>
<td>Tokyo</td>
</tr>
<tr>
<td>2</td>
<td>untrust</td>
<td>Paris Trust LAN</td>
<td>trust</td>
<td>trust</td>
<td>Tokyo Trust LAN</td>
<td>RNY any</td>
<td>permit</td>
<td>Tokyo</td>
</tr>
<tr>
<td>3</td>
<td>trust</td>
<td>Paris Trust LAN</td>
<td>untrust</td>
<td>trust</td>
<td>Tokyo Trust LAN</td>
<td>RNY any</td>
<td>permit</td>
<td>Paris</td>
</tr>
<tr>
<td>4</td>
<td>untrust</td>
<td>Tokyo Trust LAN</td>
<td>trust</td>
<td>trust</td>
<td>Paris Trust LAN</td>
<td>RNY any</td>
<td>permit</td>
<td>Paris</td>
</tr>
</tbody>
</table>

f. Click OK to save your changes to the virtual router, then click OK to save your changes to the Paris device.
EXAMPLE: CONFIGURING A POLICY-BASED SITE-TO-SITE VPN, MANUAL KEY
In this example, a Manual Key tunnel provides a secure communication channel between offices in Tokyo and Paris, using ESP with 3DES encryption and SHA-1 authentication. The Trust zones at each site are in NAT mode. The Trust and Untrust security zones and the Untrust-Tun tunnel zones are in the trust-vr routing domain. The Untrust zone interface (ethernet3) serves as the outgoing interface for the VPN tunnel.

To set up the tunnel, you must configure the security devices at both ends of the tunnel. First, you create the VPN components that you use to build the VPN, such as the security devices and the shared Address Objects. Next, you configure the VPN tunnel and add the necessary static routes on each device. Finally, you create VPN rules in a Security Policy to create the VPN tunnel between the two sites.

Figure 182: PB Site-to-Site VPN, MK Example Overview

1. Create VPN Components:
   - Security Devices. See “Add the Tokyo and Paris security devices (for details on adding devices, see Chapter 4, “Adding Devices”)” on page 666.
   - Address Objects. See “Create the Address Objects that you use in the VPN rule in the firewall rulebase (for details on creating VPN rules, see “Adding VPN Rules” on page 664).” on page 666.

2. Create the Tokyo VPN:
   a. In the device navigation tree, select VPN Settings > AutoKey IKE/Manual VPN.
   b. Select the Manual tab, then click the Add icon. The Properties screen appears. Configure the following:
      - For Name, enter Tokyo_Paris.
      - For Gateway, enter 2.2.2.2.
      - For Local SP, enter 3020.

4. Create the Paris VPN:
   a. In the device navigation tree, select VPN Settings > AutoKey IKE/Manual VPN.
   b. Select the Manual tab, then click the Add icon. The Properties screen appears.
   c. Configure the following:
      - For Name, enter Paris_Tokyo.
      - For Gateway, enter 2.2.2.2.
      - For Local SPI, enter 3020.
      - For Remote SPI, enter 3030.
      - For Outgoing Interface, select ethernet3.
      - For ESP/AH, select ESP CBC.
      - For Encryption Algorithm, select 3DES-CBC, then select Generate Key by Password and enter the password asdlk24234.
      - For Authentication Algorithm, select SHA-1, then select Generate Key by Password and enter the password PNas134a.
   d. Select the Binding tab. Enable Tunnel Zone and select untrust-tun.
   e. Click OK to save the new VPN.


6. Create the Security Policy:
a. In the main navigation tree, select Security Policies. Click the Add icon to display the new Security Policy dialog box.

b. Configure the following, then click OK:
   - For Security Policy Name, enter Corporate Policy-Based VPN.
   - Enter comments, if desired.

c. In the main navigation tree, select Security Policies > Corporate Policy-Based VPN. The security policy appears in the main display area. Configure two VPN rules as shown below:

Figure 183: Configure Two VPN Rules for PB Site-to-Site VPN, MK
- Rule 1 creates the VPN tunnel from the Tokyo device to the Paris device.
- Rule 2 creates the VPN tunnel from the Paris device to the Tokyo device.

d. Save the Security Policy.

EXAMPLE: CONFIGURING A POLICY-BASED RAS VPN, L2TP
In this example, you create a RAS user group called Field Sales and configure an L2TP tunnel called Sales_Corp, using ethernet3 (Untrust zone) as the outgoing interface for the L2TP tunnel. The security device applies the default L2TP tunnel settings to the RAS user group.

NOTE: An L2TP-only configuration is insecure and is recommended only for debugging.

The remote L2TP clients are on Windows 2000 operating systems. For information on how to configure L2TP on the remote clients, refer to Windows 2000 documentation. Only the configuration for the security device end of the L2TP tunnel is provided below.

Figure 184: PB RAS VPN, L2TP Example Overview

1. Configure the L2TP user objects:
   a. Configure an L2TP user object for Adam, then click OK:
      - For Name, enter Adam.
      - Select Enable, then select L2TP.
      - Select Password, then enter and confirm the password: AjbioJ15.
   
   b. Configure an L2TP user object for Betty, then click OK:
      - For Name, enter Betty.
      - Select Enable, then select L2TP.
Device-Level VPN Examples

Chapter 10: Configuring VPNs

2. Create a local user group called Field Sales that includes the Adam, Betty, and Carol local user objects. For details on creating a local user group, see “Configuring User Objects” on page 507.

3. Configure the Remote Settings object. Configure the following, then click OK:

- For Name, enter RM_L2TP.
- For Color, select green.
- For Dns1, enter 1.1.1.2.
- For Dns2, enter 1.1.1.3.
- For Wins1, enter 0.0.0.0.
- For Wins2, enter 0.0.0.0.

For details on creating Remote Settings objects, see “Configuring Remote Settings” on page 515.

4. Configure the IP Pool object. Configure the following, then click OK:

- For IP Pool Name, enter Global.
- For Color, select magenta.
- For Start IP, enter 10.10.2.100.
- For End IP, enter 10.10.2.180.

For details on creating IP Pool objects, see “Configuring IP Pools” on page 511.

5. Configure the L2TP tunnel:

a. In Device Manager, double-click the device icon for the device on which you want to configure the L2TP tunnel.

b. In the device navigation tree, select VPN Settings > L2TP. In the main display area, click the Add icon. The null-L2TP tunnel dialog box appears.

c. Configure the following, then click OK:

- For Name, enter Sales_Corp.
- For Outgoing Interface, select ethernet3.
- For Keep Alive, enter 60.
- For Peer IP, enter 0.0.0.0 (because the peer’s ISP dynamically assigns it an IP address, enter 0.0.0.0 here).
- Select Use Custom Settings, and leave the default authentication server as Local.
- For User/Group, select Dialup Group, then select Field Sales.

d. Click OK to save your changes to the device.

6. Configure a rule in the Zone Rulebase of a Security Policy, as shown below:

Figure 185: Configure Rule for PB RAS VPN, L2TP

<table>
<thead>
<tr>
<th>No.</th>
<th>Match</th>
<th>Action</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>From Zone: untrust</td>
<td></td>
<td>Chicago</td>
</tr>
<tr>
<td></td>
<td>Source: Dial-Up VPN trust</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>To Zone: any</td>
<td>Destination: any Service: tunnel</td>
<td>L2TP Tunnel: Sales_Corp</td>
</tr>
</tbody>
</table>

**Configure VPN**

- Device: Chicago
- VPN Type: L2TP VPN
- L2TP Tunnel: Sales_Corp
- VPN Tunnel (for L2TP-Over-IPSec): none
- None: Source is RAS
- Select Destination Addresses
  - Address
  - Global MIP
  - Global VIP
Part 4
Monitoring

The chapters in Part 4 of the NetScreen-Security Manager 2005.3 Administrators Guide are designed to help you monitor the status of your security devices (and VPN tunnels), as well as use log entries and reports to review and ensure the efficiency of your Security Policies.

Part 4 contains the following chapters:

- Chapter 11 “Monitoring” details the firewall, VPN, and NSRP monitoring functionality of NetScreen-Security Manager.
- Chapter 12 “Logging” details how to manage, filter, and export firewall logs in the Log Viewer, how to investigate suspicious activity in the Log Investigator, and how to track administrative changes in the Audit Log Viewer.
- Chapter 13 “Reporting” details how to create reports from log information.

For additional information about specific terms, objects, or functionality referred to in this guide, see Part 5, “Appendixes” on page 801. For help in locating documentation for a term, task, or concept in this guide, see Part 6, “Index” on page 905.
Chapter 11
Monitoring

In this chapter:

- About the Realtime Monitor
- Monitoring Security Devices
- Monitoring VPNs
- Monitoring NSRP Statistics
- Using The Realtime Monitor
- Monitoring the Management System

This chapter describes how to use the Realtime Monitor module in Juniper Networks NetScreen-Security Manager to monitor the status and traffic statistics for all the managed Juniper Networks security devices in your network in real time. You can use the Realtime Monitor to monitor and track the day-to-day health and performance of your network security devices, VPN tunnels, and NSRP clusters.

It also describes how to use the Server Manager module to monitor the status of the NetScreen-Security Manager management system.

About the Realtime Monitor

The Realtime Monitor module in NetScreen-Security Manager enables you to monitor real time status and statistics about all the managed security devices, VPN tunnels, and NSRP clusters in your network at a glance. You can use the Realtime Monitor to identify problems, track security events, and discover trends across multiple geographic regions and functional areas from a central management location.

The Realtime Monitor can also help you quickly identify potential device, network, or even system-level problems, such as:

- Configuration status—At the device level, you can monitor the changing status of one or more security devices in real time.
- Connection Status—At the network level, you can monitor problems that could lead to failed devices.
- Performance—At the system level, you can monitor the activity between VPN members or NSRP cluster.

The Realtime Monitor tracks the integrity of your security perimeter by continually monitoring your security devices for security events (failed security devices, abnormal utilization, general errors). The Realtime monitor does the work of a management expert by first gathering information about specific processes and network activity, then color-coding each event to organize problems.

NOTE: If you previously implemented historical reporting in Juniper Networks Global PRO, and you want to continue generating statistical reports based on historical information, it is highly recommended that you install NetScreen-Statistical Report Server. If you choose not to install NetScreen-Statistical Report Server, you can still continue to use historical reports with NetScreen-Security Manager to track Service Level Agreement, traffic, and resource statistics on security devices running ScreenOS 4.0.x. Refer to the NetScreen-Security Manager 2004 FP2 Migration Guide for more information.

Realtime Monitor Views

The Realtime Monitor includes three views:

- Device Monitor—Displays status information on the managed security devices in your network. This includes the name and type of each security device managed in NetScreen-Security Manager, connection status, and current configuration status. From the Device Monitor, you can also access more detailed information and statistics on each security device including ScreenOS version, mode, CPU utilization, memory, sessions, and network traffic.

- VPN Monitor—Displays status information on all VPN tunnel sessions that have been implemented within the domain you are working in. From the VPN Monitor, you can determine if a VPN tunnel is up, down, or not monitored.

- NSRP Monitor—Displays status information about NSRP (NetScreen Redundancy Protocol) clusters in your network. If you implement NSRP for the purpose of deploying clusters in your Juniper Networks security system, you can use the NSRP Monitor to view and troubleshoot the status of security devices in clusters within the domain you are working in.

Monitoring Security Devices

Use the Device Monitor to get an at-a-glance view of the current status of all the managed security devices in your network.

If you have configured multiple sub-domains, you can view all your managed devices from the global domain.

Information provided by the Device Monitor includes:

- Up/down connection status of managed security devices.

- Configuration status of the security devices in NetScreen-Security Manager.
Name, type and firmware version running on the security devices managed in NetScreen-Security Manager.

Figure 186: Device Monitor Dialog Box

Viewing Device Status

The following table lists and describes the device information that you can view through the Device Monitor:

Table 33: Device Status Information

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name assigned to the security device in NetScreen-Security Manager.</td>
</tr>
<tr>
<td>Domain</td>
<td>Domain in NetScreen-Security Manager in which the security device is managed.</td>
</tr>
<tr>
<td>Device Type</td>
<td>Model number of the security device.</td>
</tr>
</tbody>
</table>

Note: If you have configured multiple sub-domains, you can view all your managed devices from the global domain.
Monitoring Security Devices

- **OS Version**: ScreenOS firmware version running on the security device.

- **Config Status**: Displays the current configuration status of the security device in NetScreen-Security Manager:
  - **None**: No state has been set (does not show in Device Monitor).
  - **Modeled**: The security device exists in NetScreen-Security Manager, but a connection to the device has not yet been established.
  - **RMA**: Equivalent to bringing the device into the Modeled state. RMA results from an admin selection in the User Interface when a security device goes down.
  - **Waiting for 1st connect**: NetScreen-Security Manager is waiting for the security device to connect. You must enter a command on the security device to make it connect to NetScreen-Security Manager.
  - **Import Needed**: You must import the configuration of the security device into NetScreen-Security Manager. When you add a security device running ScreenOS 5.x for the first time, verify that your status indicates “Import Needed” before you attempt to import the device. During migration, this state indicates that import of the security device configuration is still required.
  - **OS Version Adjustment Needed**: The firmware version detected running on the device is different than what was previously detected in NetScreen-Security Manager. This could happen in the event that the automatic adjustment option was cleared during a change device firmware directive.
  - **Update Needed**: An update to this security device is required.
  - **Managed**: The security device is currently being managed by NetScreen-Security Manager.

For devices running ScreenOS 5.1 and higher, the Device Monitor can display the following additional configuration states:

- **Managed, In Sync**: The physical device configuration is synced with the modeled configuration in NetScreen-Security Manager.
- **Managed, Device Changed**: The physical device configuration is out-of-sync with the modeled configuration in NetScreen-Security Manager. Changes were made to the physical device configuration (the configuration on the physical device is newer than the modeled configuration).
- **Managed, NSM Changed**: The modeled device configuration is out-of-sync with the physical device configuration. Changes were made to the modeled configuration (the configuration on the NetScreen-Security Manager is newer than the physical device configuration).
- **Managed, NSM and Device Changed**: Both device configurations (physical and modeled) are out-of-sync each other. Changes were made to the physical device configuration and to the modeled configuration.
Chapter 11: Monitoring

Device Polling Intervals

NetScreen-Security Manager retrieves device statistics from the physical security device. The device polling interval determines the number of seconds the Device Server waits before polling for new statistics.

To configure or view the device polling intervals, double-click the Server Manager > Servers node, then select the Device Server and click the Edit icon. Use the Device Polling tab to edit the intervals to meet your monitoring requirements:

Table 34: Device Polling Intervals

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
<th>Poll Interval (in secs)</th>
<th>Save Interval (in secs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>Details traffic, interface, zone, and system-related statistics on a specific device. Information appears in the Device Monitor.</td>
<td>300</td>
<td>300</td>
</tr>
<tr>
<td>VPN</td>
<td>Details VPN tunnels between your managed devices, including VPN tunnel status (Up, Down, Not Monitored), VPN name, VPN Type, VPN source, VPN destination, security parameter index (SPI), IP address, and protocol. Information appears in the VPN Monitor.</td>
<td>300</td>
<td>300</td>
</tr>
</tbody>
</table>
Viewing Additional Device Detail and Statistics

If a security device is up and running, you can also access additional information on the device that may help you to diagnose and troubleshoot a problem from the Device Monitor. To view additional status, you can view Device Details. For traffic-related statistics and other information, you can View Statistics.

NOTE: If a security device is never connected, the Device Detail Status and Statistics views for the device are not available.

Viewing Device Details

You can also access more specific status information related to resource usage about a security device that is up and running by viewing the Device Detail Status. To view the Device Detail Status on a particular security device, right-click the security device and select View Details or simply double-click the security device.
The following table lists and describes all the information that you can view through the Device Detail Status:

Table 35: Device Detail Status Items

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS Version</td>
<td>Indicates the ScreenOS firmware version running on the security device.</td>
</tr>
<tr>
<td>Mode</td>
<td>Current operation mode of the security device: Network Address Translation (NAT), Transparent, or Route.</td>
</tr>
<tr>
<td>Latest Reboot</td>
<td>Indicates the most recent date and time that the security device was powered off and on. You can use this information to determine how long the security device was down.</td>
</tr>
<tr>
<td>CPU Utilization</td>
<td>The percent of the CPU being used at the moment of the status snapshot.</td>
</tr>
<tr>
<td>One Min. Load</td>
<td>The percent CPU utilization average on the security device for the last 1 min.</td>
</tr>
<tr>
<td>5 Min. Load</td>
<td>The percent CPU utilization average on the security device for the last 5 mins.</td>
</tr>
<tr>
<td>15 Min. Load</td>
<td>The percent CPU utilization average on the security device for the last 15 mins.</td>
</tr>
<tr>
<td>Mem Allocated</td>
<td>The original amount of memory allocated to the security device.</td>
</tr>
<tr>
<td>Mem Left</td>
<td>The amount of allocated memory that remains after being used by the security device.</td>
</tr>
</tbody>
</table>
Viewing Device Statistics

If a security device is up and running, you can also access the Statistics view to access traffic, interface, zone, and other system-related information on the device. To view statistics on a particular security device, right-click the security device in either the Device Monitor or the Device Manager and select View Statistics. The Device Statistics Summary appears in a new window.

Device Statistics Summary

The Device Statistics Summary displays the following details:

- Details describing the security device or virtual system, for example, serial number and IP address, type, and firmware version.
- Interface information
- Device status
- Time-related statistics (such as last connect or reboot)

The following table details all the information you can view about a particular security device from the Device Statistics Summary.
Table 36: Device Statistics Summary Items

<table>
<thead>
<tr>
<th>Item</th>
<th>Displays</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>Device: Displays the name, serial number, and IP address of the security device. Vsys: Displays the serial number of the security device.</td>
</tr>
<tr>
<td>Vsys</td>
<td>The name of the virtual system (if applicable)</td>
</tr>
<tr>
<td>Version</td>
<td>The security device’s build, model, and operation mode (this is not displayed in the Vsys view).</td>
</tr>
<tr>
<td>DC IP</td>
<td>The IP Address of the Date Collector the security device is contacting (this is not displayed in the Vsys view).</td>
</tr>
<tr>
<td>Interface Information</td>
<td>The employed interfaces. For example: Trust, Untrust, and Self.</td>
</tr>
<tr>
<td>Vsys Information</td>
<td>The virtual systems associated with this security device (this is not displayed in the Vsys view).</td>
</tr>
<tr>
<td>Last Known Connect Time</td>
<td>The last time the security device connected to the Data Collector (this is not displayed in the Vsys view).</td>
</tr>
<tr>
<td>Device Status</td>
<td>Whether the security device is currently up or down (this is not displayed in the Vsys view)</td>
</tr>
<tr>
<td>Last Reboot Time</td>
<td>The last time the system was restarted (this is not displayed in the Vsys view)</td>
</tr>
<tr>
<td>Last Known Uptime</td>
<td>If the security device is down, the entry lists the last time it was up. Used to determine how long a security device was down (this is not displayed in the Vsys view).</td>
</tr>
<tr>
<td>GMT Time Offset (Hours)</td>
<td>The hour the security device is set from Greenwich Mean Time (this is not displayed in the Vsys view).</td>
</tr>
<tr>
<td>DayLight-Saving</td>
<td>If you have enabled the security device to adjust time for daylight savings.</td>
</tr>
</tbody>
</table>

Additional Device Specific Views

From the Device Statistics Summary, you can access additional information enabling you to view and monitor key traffic, interface, zone, and other system-related information on a specific security device.

The following table describes each device-specific view.

Table 37: Device Specific Views

<table>
<thead>
<tr>
<th>View Type</th>
<th>View</th>
<th>Enables you to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic</td>
<td>Policy Distribution</td>
<td>View traffic on the security device distributed by policy. Enables you to view a chart of the traffic distribution by policy.</td>
</tr>
<tr>
<td></td>
<td>Protocol Distribution</td>
<td>View traffic on the security device distributed by protocol. Enables you to view a chart of the traffic distribution by protocol.</td>
</tr>
<tr>
<td></td>
<td>VPN Distribution</td>
<td>View the up/down status and active statistics of VPNs on the security device (if applicable). Also enables you to view a chart of the VPN distribution by VPN tunnel.</td>
</tr>
</tbody>
</table>
Viewing Device Traffic Distribution

You can view statistics describing the traffic on a specific security device including how the traffic is distributed, by policy, protocol, or VPNs (if applicable). You can use this information to help you identify those policies, protocols and VPN tunnels that are most and least frequently being used on a security device.

Viewing Traffic Distribution by Security Policy

Click Policy Distribution to view security device traffic that matches the access policies configured for a security device. A bar graph appears (under the Chart tab) depicting the distribution of data by policy. The graph displays a percentage of the absolute number of bytes for the top 10 policies by default.

<table>
<thead>
<tr>
<th>View Type</th>
<th>View Type</th>
<th>View</th>
<th>Enables you to...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Interface</strong></td>
<td>Ethernet Statistics</td>
<td>View security device traffic over specific interfaces. Enables you to view a chart of the utilization distributed by interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Flow Statistics</td>
<td>View security device traffic on flow counters over specific interfaces. Enables you to view a chart of flow statistics distributed by interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Attack Statistics</td>
<td>View all of the attacks that have occurred on a security device over specific interfaces. Enables you to view a chart of attacks distributed by interface.</td>
<td></td>
</tr>
<tr>
<td><strong>Zone</strong></td>
<td>Ethernet Statistics</td>
<td>View security device traffic from specific zones. Enables you to view a chart of the traffic distributed by zone.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Flow Statistics</td>
<td>View security device traffic on flow related statistics for specific interfaces. Enables you to view a chart of flow statistics distributed by zone.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Attack Statistics</td>
<td>View all counters related to attacks that have occurred on a security device from specific zones. Enables you to view a chart of the attacks distributed by zone.</td>
<td></td>
</tr>
<tr>
<td><strong>System</strong></td>
<td>Resource Statistics</td>
<td>View CPU utilization and memory allocation statistics on the security device. Enables you to view CPU, Memory and Session Utilization trends.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Active Statistics</td>
<td>View administrator and user activities; active VPNs; and authenticated users on a security device. Also enables you to view a snapshot of the ongoing active sessions on the security device.</td>
<td></td>
</tr>
<tr>
<td><strong>HA</strong></td>
<td>NSRP Statistics</td>
<td>View NSRP statistics related to clusters created on the security device (if applicable).</td>
<td></td>
</tr>
</tbody>
</table>
The following table describes all of the information that is available from the Policy Distribution view.

Table 38: Policy Distribution Items.

<table>
<thead>
<tr>
<th>Item</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy ID</td>
<td>the unique identifier of the policy.</td>
</tr>
<tr>
<td>Source IP</td>
<td>the IP address of the host generating the session.</td>
</tr>
<tr>
<td>Source IP Mask</td>
<td>the IP address mask for the host or network generating the session.</td>
</tr>
<tr>
<td>Destination IP</td>
<td>the IP address of the host receiving the session.</td>
</tr>
<tr>
<td>Destination IP Mask</td>
<td>the IP address mask for the host or network receiving the session.</td>
</tr>
<tr>
<td>Source Zone</td>
<td>Zone of the host generating the session.</td>
</tr>
<tr>
<td>Destination Zone</td>
<td>Zone of the host receiving the session.</td>
</tr>
<tr>
<td>VPN Name</td>
<td>Name of the Virtual Private Network.</td>
</tr>
<tr>
<td>Service</td>
<td>the application or service associated with the policy. Examples include Mail, FTP, SNMP, AOL, Telnet, and LDAP.</td>
</tr>
</tbody>
</table>
Monitoring Security Devices

Adjusting Data Depicted Graphically

You can adjust all elements depicted in the graph including the policies, data values (such as absolute or delta), and type of data (bytes in or out, packets in or out, utilization).

To adjust policies depicted graphically:

1. Right-click within the chart and select Configure Policies. A dialog enabling you to select which policies to view appears.

2. Clear the Default checkbox.

3. Click to select the policies that you wish to view on the graph from the list of Available Policies. Click Add to add the policies that you want to the list of Selected Policies.

4. Click to select the policies that you no longer wish to view on the graph from the list of Selected Policies. Click Remove to remove the policies from the list of Selected Policies.

5. Click OK to apply your changes; or click Cancel to cancel your changes.

To adjust data and data types depicted graphically:

1. Right-click the Chart view.

2. From the Data option, select either Delta or Absolute.

3. From the Data Type option, select either Connections, Bytes, or Packets.

4. Click OK to apply your changes; or click Cancel to cancel your changes.

<table>
<thead>
<tr>
<th>Item</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>the activity to be performed, such as Permit, Deny, or Tunnel.</td>
</tr>
<tr>
<td>Total Connections</td>
<td>the total number of data connections.</td>
</tr>
<tr>
<td>Connection Rel%</td>
<td>the relative percentage of connections.</td>
</tr>
<tr>
<td>Delta Connection</td>
<td>the total numerical difference between the current connection value and the previous connection value.</td>
</tr>
<tr>
<td>Total Bytes</td>
<td>the total number of data bytes.</td>
</tr>
<tr>
<td>Bytes Rel%</td>
<td>the relative percentage of bytes.</td>
</tr>
<tr>
<td>Delta Bytes</td>
<td>the total numerical difference between the current bytes value and the previous bytes value.</td>
</tr>
<tr>
<td>Total Packets</td>
<td>the total number of data packets.</td>
</tr>
<tr>
<td>Packets Rel%</td>
<td>the relative percentage of packets.</td>
</tr>
<tr>
<td>Delta Packets</td>
<td>the total numerical difference between the current bytes value and the previous packets value.</td>
</tr>
<tr>
<td>Policy Name</td>
<td>name of the policy.</td>
</tr>
</tbody>
</table>
### Viewing Traffic Distribution by Protocol

Click the Protocol Distribution node to view the distribution of traffic according to the protocols flowing through the device. Protocols are predefined services (such as HTTP, SNMP, or Telnet) that are enabled for each security device. You can view up to ten protocols. A bar graph appears similar to the one presented for viewing traffic according to policy distribution. The graph displays a percentage of the absolute number of bytes for the top 10 protocols by default.

![Protocol Distribution Dialog Box](image)

#### Protocol Distribution [Data: Absolute, Data Type: Bytes In, Interface: self]

The following table describes all of the information that is available from the Protocol Distribution view:

<table>
<thead>
<tr>
<th>Item</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>the name of the predefined service (like HTTP, SNMP, or Telnet) operating on the selected interface.</td>
</tr>
<tr>
<td>Interface</td>
<td>the type of interface through which the protocol is flowing.</td>
</tr>
<tr>
<td>Bytes In</td>
<td>the number of incoming bytes for the protocol through the security device.</td>
</tr>
</tbody>
</table>
Adjusting Data Depicted Graphically

You can adjust the interfaces (such as Trust, Untrust, Management, NSRP, and Self) and data depicted graphically in the same way that you adjust the Policy Distribution graphs.

### Adjusting VPN Tunnels Depicted Graphically

1. Right-click the Chart view and select Configure VPNs. A pop-up enabling you to select VPNs appears.

<table>
<thead>
<tr>
<th>Item</th>
<th>Displays…</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bytes In Rel%</td>
<td>Relative percentage of all incoming bytes.</td>
</tr>
<tr>
<td>Delta Bytes In</td>
<td>the total numerical difference between the current bytes in value and the previous bytes in value.</td>
</tr>
<tr>
<td>Bytes Out</td>
<td>the number of outgoing bytes for the protocol through the security device.</td>
</tr>
<tr>
<td>Bytes Out Rel%</td>
<td>Relative percentage of all outgoing bytes.</td>
</tr>
<tr>
<td>Delta Bytes Out</td>
<td>the total numerical difference between the current bytes out value and the previous bytes out value.</td>
</tr>
<tr>
<td>Packets In</td>
<td>the number of incoming packets handled by the protocol through the security device.</td>
</tr>
<tr>
<td>Packets In Rel%</td>
<td>Relative percentage of all incoming packets.</td>
</tr>
<tr>
<td>Delta Packets In</td>
<td>the total numerical difference between the current packets in value and the previous packets in value.</td>
</tr>
<tr>
<td>Packets Out</td>
<td>the number of outgoing packets handled by the protocol through the security device.</td>
</tr>
<tr>
<td>Packets Out Rel%</td>
<td>Relative percentage of all outgoing packets.</td>
</tr>
<tr>
<td>Delta Packets Out</td>
<td>the total numerical difference between the current packets out value and the previous packets out value.</td>
</tr>
<tr>
<td>Util. (Absolute)</td>
<td>the total number of the utilization of the current security device.</td>
</tr>
<tr>
<td>Util. (Delta)</td>
<td>the total numerical difference between the current utilization value and the previous utilization value.</td>
</tr>
<tr>
<td>Zone</td>
<td>the name of the zone associated with the protocol.</td>
</tr>
</tbody>
</table>

### Viewing Traffic Distribution by VPN (if applicable)

If you are using your security devices to implement VPNs, you can view how traffic is being distributed across each different VPN tunnel on the security device. A bar graph appears (under the Chart tab) depicting the distribution of data traveling to and from each VPN tunnel. The graph uses a percentage of the absolute number of bytes traveling in to the top 10 VPN tunnels by default.

You can adjust all elements depicted in the graph including the VPN tunnels, data values (absolute or delta), and type of data (bytes in or out, packets in or out, utilization).

### Adjusting VPN Tunnels Depicted Graphically

1. Right-click the Chart view and select Configure VPNs. A pop-up enabling you to select VPNs appears.
2. Clear the Default checkbox.

3. Click to select the VPN tunnel that you wish to view on the graph from the list of Available VPN tunnels. Click Add to add the VPN tunnel to the list of Selected VPN tunnels.

4. Click to select the VPN tunnel that you no longer wish to view on the graph from the list of Selected VPN tunnels. Click Remove to remove the VPN tunnel from the list of Selected VPN tunnels.

5. Click OK to apply your changes; or click Cancel to cancel your changes.

Adjusting Data Depicted Graphically
1. Right-click the Chart view and select Data, and either Delta or Absolute.

2. Right-click the Chart view and select Data Type, and either Bytes In, Bytes Out, Packets In Packets Out, Utilization, Last Session Duration, Avg Latency, Availability.

3. Click OK to apply your changes; or click Cancel to cancel your changes.

Viewing VPN-specific Information
Click the VPN Monitor Table tab to view specific information about your VPN. From the VPN Monitor Table, you can view the following details about a specific VPN:

- Key details describing the VPN (such as name, Policy ID, group and user associations, VPN type).
- Security Association (SA) information.
- Total number of data over the tunnel (such as bytes in/out, packets in/out, utilization).

The following table describes all of the information that is available from the VPN Monitor Table:

Table 40: VPN Monitor Table

<table>
<thead>
<tr>
<th>Item</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>the name of the VPN.</td>
</tr>
<tr>
<td>VPN Type</td>
<td>Type of tunnel: Site-to-site or dial-up.</td>
</tr>
<tr>
<td>SA Id</td>
<td>the Security Association (SA) identification for the VPN at both ends of the tunnel.</td>
</tr>
<tr>
<td>Policy Id-In/Out</td>
<td>A unique identifier specified when the policy was configured.</td>
</tr>
<tr>
<td>Status</td>
<td>up/down status of the VPN tunnel.</td>
</tr>
<tr>
<td>SA Status</td>
<td>whether or not the current SA has been established.</td>
</tr>
<tr>
<td>Time-SA Status Change</td>
<td>time that the SA status last changed</td>
</tr>
<tr>
<td>Last SA Session Duration</td>
<td>duration of last SA session</td>
</tr>
<tr>
<td>Group</td>
<td>Group associated with the VPN.</td>
</tr>
<tr>
<td>User</td>
<td>User associated with the VPN.</td>
</tr>
</tbody>
</table>
Viewing Active VPN Information

click the Active VPN tab to view specific information about your active VPNs. From the Active VPN, you can view the following details about your active VPNs:

- Key details describing the VPN (name, Policy IP, local and peer gateway IDs and IP addresses).
- Security established on the active VPN.
- Time-related statistics (such as lifetime, latency).

The following table describes all of the information that is available from the active VPN:

<table>
<thead>
<tr>
<th>Item</th>
<th>Displays</th>
</tr>
</thead>
<tbody>
<tr>
<td>DN Name</td>
<td>Distinguished Name (DN) of the VPN.</td>
</tr>
<tr>
<td>Avg. Latency</td>
<td>A rolling average of latency, presented in milliseconds.</td>
</tr>
<tr>
<td>Availability</td>
<td>Percentage of the time a tunnel is up over the last thirty samples.</td>
</tr>
<tr>
<td>Bytes In</td>
<td>the number of incoming bytes handled by the protocol through the security device.</td>
</tr>
<tr>
<td>Delta Bytes In</td>
<td>Total numerical difference between the current bytes in value and the previous bytes in value.</td>
</tr>
<tr>
<td>Bytes Out</td>
<td>the number of outgoing bytes handled by the protocol through the security device.</td>
</tr>
<tr>
<td>Delta Bytes Out</td>
<td>Total numerical difference between the current bytes out value and the previous bytes out value.</td>
</tr>
<tr>
<td>Packets In</td>
<td>the number of incoming packets handled by the protocol through the security device.</td>
</tr>
<tr>
<td>Delta Packets In</td>
<td>Total numerical difference between the current packets in value and the previous packets in value.</td>
</tr>
<tr>
<td>Packets Out</td>
<td>the number of outgoing packets handled by the protocol through the security device.</td>
</tr>
<tr>
<td>Delta Packets Out</td>
<td>Total numerical difference between the current packets out value and the previous packets out value.</td>
</tr>
<tr>
<td>Util. (Absolute)</td>
<td>Total number of the utilization of the current security device.</td>
</tr>
<tr>
<td>Util. (Delta)</td>
<td>Total numerical difference between the current utilization value and the previous utilization value.</td>
</tr>
</tbody>
</table>

Table 41: Active VPN Table
You can also view traffic information as it is processed by a device on a specific interface:

- Viewing Ethernet Statistics
- Viewing Flow Statistics
- Viewing Attack Statistics

**Viewing Ethernet Statistics**

Click the Ethernet Statistics node to view traffic information as it is processed by a specific physical interface on a security device. Depending upon the specific security device, the following interfaces apply:

- Trust and Untrust interfaces available on all security devices.

<table>
<thead>
<tr>
<th>Item</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability</td>
<td>Percentage of the time a tunnel is available over the last thirty samples.</td>
</tr>
<tr>
<td>Local GW Id</td>
<td>the local gateway Id for the active VPN.</td>
</tr>
<tr>
<td>Peer GW Id</td>
<td>the peer gateway Id address for the active VPN.</td>
</tr>
<tr>
<td>Local GW IP</td>
<td>the local gateway IP address for the active VPN.</td>
</tr>
<tr>
<td>Peer GW IP</td>
<td>the peer gateway IP address for the active VPN.</td>
</tr>
<tr>
<td>Local Address</td>
<td>the local IP address for the security device associated to the active VPN.</td>
</tr>
<tr>
<td>Peer Address</td>
<td>the peer IP address for the security device connected to the active VPN.</td>
</tr>
<tr>
<td>Monitor</td>
<td>whether a monitoring capability for the VPN is ON or OFF.</td>
</tr>
<tr>
<td>IPSec</td>
<td>the IPSec (IP security) protocol for the active VPN; for example, AH (Authentication Header) or ESP (Encapsulating Security Payload).</td>
</tr>
<tr>
<td>SPI In</td>
<td>the SPI (Security Parameter Index) key into the active VPN. This is an encryption method.</td>
</tr>
<tr>
<td>SPI Out</td>
<td>the SPI (Security Parameter Index) key out of the active VPN. This is an encryption method.</td>
</tr>
<tr>
<td>Encryption</td>
<td>Algorithm used when a user encrypts communication between the security device and the server. Listed as either SDI or DES.</td>
</tr>
<tr>
<td>Authentication</td>
<td>A second algorithm used when a user encrypted communication between the security device and the server.</td>
</tr>
<tr>
<td>Key</td>
<td>Type of key associated with the VPN: Auto IKE (Internet Key Exchange) or manual key.</td>
</tr>
<tr>
<td>Lifetime P1</td>
<td>Time listed in seconds before re-keying.</td>
</tr>
<tr>
<td>Lifetime P2</td>
<td>Time reported in remaining bytes before re-keying. Independent from Lifetime P1.</td>
</tr>
<tr>
<td>Life Size</td>
<td>the predefined duration of the tunnel (in bytes).</td>
</tr>
<tr>
<td>P1 Status</td>
<td>whether the P1 (phase 1) status for tunnel negotiation is enabled/disabled.</td>
</tr>
<tr>
<td>P2 Status</td>
<td>whether the P2 (phase 2) status for tunnel negotiation is enabled/disabled.</td>
</tr>
<tr>
<td>P1 Auth</td>
<td>Associated with Auto IKE. This column displays the P1 (phase 1) authentication for the active VPN.</td>
</tr>
</tbody>
</table>
DMZ interface available on NetScreen-25, NetScreen-50, NetScreen-100 and NetScreen-500 devices; the NetScreen-5XP device has no DMZ interface.

HA interface and management interface available on NetScreen-100 and NetScreen-500 devices.

Ethernet Statistics apply only to security devices, and not to virtual systems.

A graph appears displaying security device % utilization traffic on the interface. Right-click within the chart to select a desired Interface (such as Ethernet or HA). The active interface is listed below the graph. The graph will also provide the total errors in a graphical form. You can view up to 12 samples in the chart. The following table describes the information available from the Ethernet Statistics view:

**Table 42: Ethernet Statistics View Data**

<table>
<thead>
<tr>
<th>Item</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>the data for each interface.</td>
</tr>
<tr>
<td>Bytes In</td>
<td>the number of bytes of incoming traffic processed through the security device over the selected interface.</td>
</tr>
<tr>
<td>Delta Bytes In</td>
<td>the total numerical difference between the current bytes in value and the previous bytes in value.</td>
</tr>
<tr>
<td>Bytes Out</td>
<td>the number of outgoing bytes handled by the interface through the security device.</td>
</tr>
<tr>
<td>Delta Bytes Out</td>
<td>the total numerical difference between the current bytes out value and the previous bytes out value.</td>
</tr>
<tr>
<td>Packets In</td>
<td>the number of incoming packets handled by the interface through the security device.</td>
</tr>
<tr>
<td>Delta Packets In</td>
<td>the total numerical difference between the current packets in value and the previous packets in value.</td>
</tr>
<tr>
<td>Packets Out</td>
<td>the number of outgoing packets handled by the interface through the security device.</td>
</tr>
<tr>
<td>Delta Packets Out</td>
<td>the total numerical difference between the current packets out value and the previous packets out value.</td>
</tr>
<tr>
<td>Broadcast</td>
<td>the number of broadcast-type packets processed through the security device over the selected interface.</td>
</tr>
<tr>
<td>CRC Errors</td>
<td>the number of packets generating a cyclic redundancy code error processed through the security device over the selected interface.</td>
</tr>
<tr>
<td>Alignment Errors</td>
<td>the number of Frame Checksum (FCS) errors.</td>
</tr>
<tr>
<td>ShortFrame</td>
<td>the number of frames that are not of the correct length.</td>
</tr>
<tr>
<td>RXCollision</td>
<td>the number of times that two packets collide, resulting in damage to both. This indicates that the network is overloaded.</td>
</tr>
<tr>
<td>Speed (Mbps)</td>
<td>This is useful in calculating the speed of the interface.</td>
</tr>
<tr>
<td>Status</td>
<td>whether the security device is currently Up or Down.</td>
</tr>
<tr>
<td>Direction</td>
<td>whether the security device is in half or full duplex mode.</td>
</tr>
<tr>
<td>Zone</td>
<td>the name of the zone associated with the interface.</td>
</tr>
</tbody>
</table>
Viewing Flow Statistics

Click the Flow Statistics node to view data for various flow counters on a specific security device or virtual interface. For each security device, the data and statistics are separated by all available interfaces.

You can change the interface setting by right-clicking in the chart and selecting the interface that you want. The following table describes all of the information that is available from the Flow Statistics view:

Table 43: Flow Statistics View Data

<table>
<thead>
<tr>
<th>Item</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>the name of the virtual interface.</td>
</tr>
<tr>
<td>Bytes In</td>
<td>the number of bytes of incoming traffic processed through the security device over the selected interface.</td>
</tr>
<tr>
<td>Bytes Out</td>
<td>the number of bytes of outgoing traffic processed through the security device over the selected interface.</td>
</tr>
<tr>
<td>Packets In</td>
<td>the number of incoming packets processed through the security device over the selected interface.</td>
</tr>
<tr>
<td>Packets Out</td>
<td>the number of outgoing packets processed through the security device over the selected interface.</td>
</tr>
<tr>
<td>VLAN In</td>
<td>the number of VLAN packets received through the security device; applies to virtual systems.</td>
</tr>
<tr>
<td>VLAN Out</td>
<td>the number of VLAN packets sent through the security device; applies to virtual systems.</td>
</tr>
<tr>
<td>Connections</td>
<td>the number of connections that occurred for a given interface.</td>
</tr>
<tr>
<td>Packets Dropped</td>
<td>the number of incoming packets dropped by a given interface.</td>
</tr>
<tr>
<td>Packets Denied</td>
<td>the number of incoming packets denied on the virtual interface by the policy.</td>
</tr>
<tr>
<td>Authentication Failed</td>
<td>the number of packets dropped because of an authentication failure.</td>
</tr>
<tr>
<td>URL Blocking Dropped</td>
<td>the number of packets dropped because of URL blocking.</td>
</tr>
<tr>
<td>IPSec Dropped</td>
<td>the number of IPSec packets dropped.</td>
</tr>
<tr>
<td>Zone</td>
<td>the name of the zone associated with the interface.</td>
</tr>
</tbody>
</table>

Viewing Attack Statistics

Click the Attack Statistics node to view distribution of the attacks that have occurred on a specific security device. The report separates the data and statistics for all available interfaces. The following table describes each of the attack counters available from the Attack Statistics view:

Table 44: Attack Counters

<table>
<thead>
<tr>
<th>Item</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Name of the interface.</td>
</tr>
<tr>
<td>SYN Attack</td>
<td>SYN packets overwhelm a network by initiating so many connection attempts or information requests that the network can no longer process legitimate connection requests, resulting in a Denial of Service.</td>
</tr>
<tr>
<td>Item</td>
<td>Displays...</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Tear Drop</td>
<td>When the first and second parts of a fragmented packet overlap, the server attempting to reassemble the packet can crash. If the security device sees this discrepancy in a fragmented packet, it drops the packet.</td>
</tr>
<tr>
<td>Source Route</td>
<td>This option applies in an IP header and allows an attacker to enter a network with a false IP address and have data sent back to the attacker’s real address.</td>
</tr>
<tr>
<td>Ping of Death</td>
<td>Intentionally oversized or irregular ICMP packets can trigger a Denial of Service condition, freezing, or other adverse system reactions. You can configure a security device to detect and reject oversized or irregular packet sizes.</td>
</tr>
<tr>
<td>Address Spoofing</td>
<td>You can enable a security device to guard against spoofing attacks by checking its own route table. If the IP address is not in the route table, traffic through the security device is not allowed.</td>
</tr>
<tr>
<td>Land Attack</td>
<td>Combining a SYN attack with IP spoofing, a Land attack occurs when an attacker sends spoofed SYN packets containing the IP address of the victim as both the destination and source IP address. This creates an empty connection. Flooding a system with such empty connections can overwhelm the system, causing a Denial of Service. Security devices automatically block any attempt of this nature and records such attempts as a Land attack.</td>
</tr>
<tr>
<td>ICMP Flood</td>
<td>ICMP pings can be so numerous that they overload a system with so many echo requests that the system expends all its resources responding until it can no longer process valid network traffic. If you set a threshold to invoke ICMP flood attack protection when exceeded, ICMP flood attacks are recorded as statistics.</td>
</tr>
<tr>
<td>UDP Flood</td>
<td>Similar to the ICMP flood, UDP flooding occurs when UDP packets are sent with the purpose of slowing down the system to the point that it can no longer handle valid connections. After enabling the UDP flood protection feature, you can set a threshold that once exceeded invokes the UDP flood attack protection feature. (The default threshold value is 1000 packets per second.) If the threshold is exceeded, the security device ignores further UDP packets for the remainder of that second.</td>
</tr>
<tr>
<td>Port Scan</td>
<td>Port scan attacks occur when packets are sent with different port numbers with the purpose of scanning the available services in hopes that one port will respond. The security device internally logs the number of different ports scanned from one remote source. If a remote host scans 10 ports in 0.3 seconds, Juniper Networks flags this as a port scan attack, and rejects further packets from the remote source.</td>
</tr>
<tr>
<td>IP Sweep</td>
<td>This is the same as an address sweep attack, and similar to a port scan attack. It occurs when an attacker sends ICMP echo requests (or pings) to different destination addresses hoping that one will reply, thus uncovering an address to a target. If a remote host pings 10 addresses in 0.3 seconds, the security device flags this as an address sweep attack and drops the connection.</td>
</tr>
<tr>
<td>Block Java/ActX</td>
<td>Malicious Java or ActiveX components can be hidden in Web pages. When downloaded, these applets install a Trojan horse on your computer. Similarly, Trojan horses can be hidden in compressed files such as .zip, .gzip, and .tar, and executable (.exe) files.</td>
</tr>
</tbody>
</table>
### Monitoring Security Devices

#### Chapter 11: Monitoring

<table>
<thead>
<tr>
<th>Item</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYN Frag</td>
<td>A SYN fragment attack floods the target host with SYN packet fragments. The host catches the fragments, waiting for the remaining packets to arrive so it can reassemble them. By flooding a server or host with connections that cannot be completed, the host’s memory buffer eventually fills. No further connections are possible, and damage to the host’s operating system can occur. The security device drops ICMP packets when the protocol field indicates ICMP packets, and the fragment flag is set to 1 or an offset is indicated.</td>
</tr>
<tr>
<td>TCP no Flag</td>
<td>TCP packet that does not have any bits set in the flags.</td>
</tr>
<tr>
<td>Unknown Prot</td>
<td>The security device drops packets where the protocol field is set to 101 or greater. These protocol types are reserved and undefined at this time.</td>
</tr>
<tr>
<td>Bad IP Opt</td>
<td>Triggered when the list of IP options in the IP datagram header is incomplete or malformed.</td>
</tr>
<tr>
<td>IP Rec Route</td>
<td>The security device blocks packets where the IP option is 7 (Record Route). This option is used to record the route of a packet. A recorded route is composed of a series of internet addresses, which an outsider can analyze to learn details about your network’s addressing scheme and topology.</td>
</tr>
<tr>
<td>IP Timestamp</td>
<td>The security device blocks packets where the IP option list includes option 4 (Internet Timestamp).</td>
</tr>
<tr>
<td>IP Security</td>
<td>This option provides a way for hosts to send security, compartmentation, TCC (closed user group) parameters, and Handling Restriction Codes compatible with DOD requirements.</td>
</tr>
<tr>
<td>IP Loose Src</td>
<td>The security device blocks packets where the IP option is 3 (Loose Source Routing). This option provides a means for the source of a packet to supply routing information to be used by the gateways in forwarding the packet to the destination. This option is a loose source route because the gateway or host IP is allowed to use any route of any number of other intermediate gateways to reach the next address in the route.</td>
</tr>
<tr>
<td>IP Strict Src</td>
<td>The security device blocks packets where the IP option is 9 (Strict Source Routing). This option provides a means for the source of a packet to supply routing information to be used by the gateways in forwarding the packet to the destination. This option is a strict source route because the gateway or host IP must send the datagram directly to the next address in the source route, and only through the directly connected network indicated in the next address to reach the next gateway or host specified in the route.</td>
</tr>
<tr>
<td>IP Stream</td>
<td>The security device blocks packets where the IP option is 8 (Stream ID). This option provides a way for the 16-bit SATNET stream identifier to be carried through networks that do not support the stream concept.</td>
</tr>
<tr>
<td>ICMP Frag</td>
<td>When the protocol field indicates ICMP packets, and the fragment flag is set to 1 or an offset is indicated.</td>
</tr>
<tr>
<td>Large ICMP</td>
<td>An ICMP packet with a length greater than 1024.</td>
</tr>
<tr>
<td>SYN n FIN</td>
<td>Both the SYN and FIN flags are not normally set in the same packet. However, an attacker can send a packet with both flags set to see what kind of system reply is returned and thereby determine what kind of system is on the receiving end. The attacker can then use any known system vulnerabilities for further attacks. Enable this option to have the security device drop packets that have both the SYN and FIN bits set in the flags field.</td>
</tr>
<tr>
<td>FIN no ACK</td>
<td>TCP packet with a FIN set but no ACK set in the flags field.</td>
</tr>
<tr>
<td>Mal URL</td>
<td>When you enable Malicious URL Detection, the security device monitors each HTTP packet and detects any URL that matches any of several user-defined patterns. The security device automatically drops any such packet.</td>
</tr>
</tbody>
</table>
Viewing Zone Statistics
You can also view traffic information as it is processed by a security device over specific zones. You can view ethernet statistics, flow statistics and attack statistics in the same manner that you viewed them in the Interface reports according to zone.

Viewing System Statistics
You can also view system-related information for a security device.

Viewing Resource Statistics
Click the Resource Statistics node to view the resources for a security device. The following table describes all of the information that is available from the Resource Statistics view:

Table 45: Resource Statistics Items

<table>
<thead>
<tr>
<th>Item</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avg. CPU Utilization</td>
<td>the average CPU usage of the security device.</td>
</tr>
<tr>
<td>Memory Allocated</td>
<td>the current memory allocation to security device.</td>
</tr>
<tr>
<td>Memory Left</td>
<td>the remaining usable memory.</td>
</tr>
<tr>
<td>No. of Fragment Blocks</td>
<td>a percentage of blocks that are fragmented.</td>
</tr>
<tr>
<td>Active Sessions</td>
<td>the number of currently active sessions.</td>
</tr>
<tr>
<td>Allocated Sessions</td>
<td>the number of allocated sessions.</td>
</tr>
<tr>
<td>Max. Sessions Allowed</td>
<td>the maximum sessions allowed.</td>
</tr>
<tr>
<td>Failed Sessions</td>
<td>the number of sessions that failed to allocate (after maximum reached).</td>
</tr>
</tbody>
</table>
Viewing Active Statistics

click the Active Statistics node to view administrator and user activities for a security device. The Administrators tab displays information about the administrators including, when, where and how they logged in to the system. The following table describes all of the information that is available from the Administrators view:

Table 46: Administrators View

<table>
<thead>
<tr>
<th>Item</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator ID</td>
<td>the administrator’s logon ID.</td>
</tr>
<tr>
<td>IP Address</td>
<td>the administrator’s IP address.</td>
</tr>
<tr>
<td>Service Used</td>
<td>the type of service, for example, Console, Web, or Telnet to login.</td>
</tr>
<tr>
<td>Time</td>
<td>the time that the administrator logged on.</td>
</tr>
</tbody>
</table>

The following table describes all of information that is available from the Authenticated Users view:

Table 47: Authenticated Users View

<table>
<thead>
<tr>
<th>Item</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID</td>
<td>User log in ID.</td>
</tr>
<tr>
<td>Source IP Address</td>
<td>Source IP address.</td>
</tr>
<tr>
<td>Time</td>
<td>Time that the user logged on.</td>
</tr>
</tbody>
</table>

You can also access VPN information from the Active VPN view, and Active Session information from the Active Sessions view.

Viewing Active Sessions

You can view a snapshot of ongoing active sessions on the security device. You can view active sessions from the Active Statistics view.

When you click the Active Sessions tab, a short form view of the active sessions appears enabling you to monitor basic information (such as source IP, destination IP, translated IP (if applicable), source port, destination port, translated port (if applicable), policy ID, time the session starts, and protocol type) about the active sessions on the security device by default. You can also view extended information about the session, such as session ID, icmp type (if applicable), total incoming bytes, total outgoing bytes, total packets count, how long the session has been active.

The following table describes all of the information that is available from the Active Sessions view:

Table 48: Active Sessions Items

<table>
<thead>
<tr>
<th>Item</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session ID</td>
<td>A unique identifier specified with the active session.</td>
</tr>
<tr>
<td>Source IP</td>
<td>IP address of the sending node of the connection.</td>
</tr>
</tbody>
</table>
Using the Session Filter

You can control the information that is provided in the Active Sessions view by configuring a session filter. Using the Session Filter, you can fetch specific sessions on a security device that match specific criteria that you set. Like the Monitor Filter for the Event Summary View, there is only one Session Filter and it defines the overall data set that you can view from the Active Sessions view. After you have configured and applied the Session Filter, you can then configure additional session display filters to view more specific session information.

Configuring the Session Filter

To configure the session filter:

1. Use the Options menu, and select Session Filter. The Session Filter Dialog will appear.

2. Click in the Long Form checkbox to display additional information about the Active Session.

3. Click in the Maximum number of sessions to retrieve checkbox and enter the total number of sessions you want the Session Filter to retrieve.

4. Specify criteria for the sessions that you would like to view. You can specify an active session according to the following:

   - Source, Destination, and Translated IP (IP Address, Net Mask, and Port Range)
   - Session Duration
   - Session Start Date and Time
- Policy ID
- Session Type
- Protocol ID
- Policy with Logging

5. Click More to view additional criteria.

6. Click Reset to Default to reset all criteria back to their default settings.

7. Click OK when you are done.

8. Click Refresh to apply the criteria to the active session table view.

**Configuring a Session Display Filter**

You can apply a session display filter to view only specific active sessions.

1. Use the Options menu, and select Session Display Filter. The Session Filter Dialog will appear.

2. From the Source tab, you can specify the sessions that you want to view according to the Source IP Address and Port number, or Port Range.

3. Click in the Destination tab to specify the sessions that you want to view according to Destination IP Address and Port number, or Port Range.

4. Click in the Translated tab to specify the sessions that you want to view according to Translated IP Address and Port number, or Port Range.

5. Click in the Protocol tab specify the sessions that you want to view according to protocol.

6. Click in the Other tab specify the sessions that you want to view according to Session Duration, Session Start Time or Policy ID.

7. Click OK when you are done.

8. Click Refresh to apply the Session Display criteria to the active session table view.
Troubleshooting
From the Device Monitor, you can right-click on any security device and use the Troubleshoot option to query on the status of a security device using Telnet or a Secure Command Shell. You can use this capability to issue a “get” Telnet command to a security device or a CLI command to the SCS (Secure Command Shell) on the security device to troubleshoot problems.

NOTE: Commands from NetScreen-Security Manager originate from the UI client to the security device. If you intend to issue get commands from NetScreen-Security Manager, you must plan and implement Security Policy rules in your network accordingly.

Viewing High Availability (HA) Statistics (if applicable)
If you have configured security devices to be highly available, you can view NSRP-related statistics on the device by accessing the HA Statistics view. The following table describes all of the information that is available from the HA Statistics view:

Table 49: HA Statistics View

<table>
<thead>
<tr>
<th>Item</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>VSD Group ID</td>
<td>the group ID that is associated with the VSD (or RTO).</td>
</tr>
<tr>
<td>Number of Units</td>
<td>the number of units associated with the VSD (or RTO).</td>
</tr>
<tr>
<td>State Change Counter</td>
<td>the number of times a security device changes operational states.</td>
</tr>
<tr>
<td>Init Counter</td>
<td>the transient state of a VSD (or RTO) group member while it was in the process of joining the VSD (or RTO) group.</td>
</tr>
<tr>
<td>Master</td>
<td>the number of Master security devices.</td>
</tr>
<tr>
<td>Primary BackUp</td>
<td>the number of primary backup security devices.</td>
</tr>
<tr>
<td>BackUp</td>
<td>the total number of backup security devices.</td>
</tr>
<tr>
<td>Ineligible</td>
<td>Notes that an administrator purposefully assigned a security device so that it cannot participate in the selecting a new master security device.</td>
</tr>
<tr>
<td>InOperable</td>
<td>Notes that a VSD (or RTO) group security device has an internal problem.</td>
</tr>
<tr>
<td>Master Conflict</td>
<td>the number of conflicts that occurred on the master security device.</td>
</tr>
<tr>
<td>Primary Backup Conflict</td>
<td>the number of conflicts that occurred on the primary backups security device.</td>
</tr>
<tr>
<td>Tx Heartbeat</td>
<td>the number of transmitted heartbeats on the security devices.</td>
</tr>
<tr>
<td>Rx Heartbeat</td>
<td>the number of received heartbeats on the security devices.</td>
</tr>
</tbody>
</table>

Monitoring VPNs
Use VPN Monitor to get an at-a-glance status of the up/down status of VPN tunnels as well as other statistics relevant to your VPN.
Monitoring VPNs

Chapter 11: Monitoring

Figure 191: Monitoring VPNs

The VPN Monitor lists a summary of all the VPN tunnels that have been implemented in your system. It includes visual indicators that depict whether an existing VPN tunnel is either Up, Down, or Not Monitored. The Summary also includes information describing the VPN name, VPN type, Source, Destination, Security Parameter Index, IP Address, and Protocol.

Table 50: VPN Tunnel Summary

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN</td>
<td>Name of the active VPN.</td>
</tr>
<tr>
<td>VPN Type</td>
<td>Type of tunnel: Dialup or Site to Site.</td>
</tr>
<tr>
<td>From Hostname/(IP)/(Vsys)</td>
<td>Source security devices used in the VPN. For example, a root security device named NS5000 with an IP address of 1.1.1.1 appears as NS5000(1.1.1.1). For a Vsys 1, “NS5000(1.1.1.1)(1)” appears.</td>
</tr>
<tr>
<td>From Domain</td>
<td>Domain in NetScreen-Security Manager in which the source security device used in the VPN is managed.</td>
</tr>
<tr>
<td>To Hostname/(IP)/(Vsys)</td>
<td>Destination security devices used in the VPN. For example, a root security device named NS5000 with an IP address of 1.1.1.1 appears as NS5000(1.1.1.1). For a Vsys 1, “NS5000(1.1.1.1)(1)” appears.</td>
</tr>
<tr>
<td>To Domain</td>
<td>Domain in NetScreen-Security Manager in which the destination security device used in the VPN is managed.</td>
</tr>
<tr>
<td>Status</td>
<td>VPN Status: Up or Down</td>
</tr>
<tr>
<td>SPI (in/out)</td>
<td>Security Parameter Index (SPI) key into and out of the active VPN. This is the encryption method.</td>
</tr>
</tbody>
</table>

NOTE: You must enable the “VPN Monitor” option on the tunnel when configuring the tunnel for the device.

Viewing the VPN Status Summary

The VPN Monitor lists a summary of all the VPN tunnels that have been implemented in your system. It includes visual indicators that depict whether an existing VPN tunnel is either Up, Down, or Not Monitored. The Summary also includes information describing the VPN name, VPN type, Source, Destination, Security Parameter Index, IP Address, and Protocol.
Configuring a VPN Display Filter

You can control the information that is provided in the VPN Monitor by configuring a VPN display filter. Use the Options menu and select Display Filter to configure a VPN display filter. The VPN Display filter provides several options enabling you to view VPN information related to the type, status, or the specific security device or virtual system associated with the VPN tunnel that you want to view. Click the Refresh button to apply the Session Display criteria to the active session table view.

Viewing Active VPN Details

To view the details on the active VPN, click to select the VPN, use the View menu and select Active VPN Details (alternatively, you can also right-click the VPN tunnel and select Active VPN Details).

Refer to “Viewing Active VPN Information” on page 696 for more information on the Active VPN Details table.

Viewing Device-Specific VPN Information

Right-click the VPN tunnel and select Monitor Data, and then the security device to view security device-specific information about your VPN. A Monitor info window appears where you can access the VPN Monitor table, Active VPN table, and a chart enabling you to view the distribution of VPN tunnels on the security device.

Monitoring NSRP Statistics

If you have implemented NetScreen Redundancy Protocol (NSRP) for the purpose of deploying clusters for redundancy, you can use the NSRP Monitor to get an at-a-glance status of your Juniper Networks systems that are in “clusters.” These systems include both the NetScreen-500 and the NetScreen-1000. To launch the NSRP Monitor, click NSRP Monitor.

Viewing NSRP Summary Information

Double-click an NSRP device to view a summary of the top-level information on the selected cluster. From the NSRP Summary, you can view the following details about a specific cluster:

- Key details describing the cluster (such as name, # of VSDs, # of RTOs)
- Security details
- The total number and type of events

The following table describes all of the information that is available from the NSRP summary:

<table>
<thead>
<tr>
<th>IP (Local-Peer)</th>
<th>Peer gateway IP address for the active VPN.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>Protocol used for the active VPN</td>
</tr>
<tr>
<td>Peer GW ID</td>
<td>Peer gateway ID for the active VPN.</td>
</tr>
</tbody>
</table>
Table 51: NSRP Device Summary

<table>
<thead>
<tr>
<th>Item</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster</td>
<td>name of this cluster.</td>
</tr>
<tr>
<td>Domain</td>
<td>Domain in NetScreen-Security Manager in which the NSRP device is managed.</td>
</tr>
<tr>
<td>No of VSD’s</td>
<td>the total number of Virtual security devices (VSD) that are attached to this cluster.</td>
</tr>
<tr>
<td>No of RTO’s</td>
<td>the total number of Run Time Objects (RTO) that are attached to this cluster.</td>
</tr>
<tr>
<td>Encryption</td>
<td>whether or not encryption has been enabled/disabled.</td>
</tr>
<tr>
<td>Authentication</td>
<td>whether or not authentication has been enabled/disabled.</td>
</tr>
<tr>
<td>No. of Gratuitous arps</td>
<td>the number of gratuitous arps.</td>
</tr>
<tr>
<td>Critical Events</td>
<td>the total number of Critical events that occurred.</td>
</tr>
<tr>
<td>Major Events</td>
<td>the total number of Major events that occurred.</td>
</tr>
<tr>
<td>Minor Events</td>
<td>the total number of Minor events that occurred.</td>
</tr>
<tr>
<td>Warning Events</td>
<td>the total number of Warning events that occurred.</td>
</tr>
<tr>
<td>Intermediate Events</td>
<td>the total number of Intermediate events that occurred.</td>
</tr>
<tr>
<td>Clear Events</td>
<td>the total number of Clear events that occurred.</td>
</tr>
<tr>
<td>Cluster</td>
<td>the name of the cluster associated with this VSD.</td>
</tr>
<tr>
<td>VSD(RTO)</td>
<td>the name of this VSD (or RTO).</td>
</tr>
<tr>
<td>No of Devices</td>
<td>the total number of security devices that are associated with this VSD.</td>
</tr>
<tr>
<td>Init Hold Time (sec)</td>
<td>the initial hold time state (in seconds) of the VSD.</td>
</tr>
<tr>
<td>Heartbeat Interval (ms)</td>
<td>the time interval (in milliseconds) between each heartbeat.</td>
</tr>
<tr>
<td>Heartbeat Lost Threshold (ms)</td>
<td>threshold level required to change over to the backup security device.</td>
</tr>
<tr>
<td>Master</td>
<td>the Master System.</td>
</tr>
<tr>
<td>Primary Backup</td>
<td>the Primary System.</td>
</tr>
</tbody>
</table>

Viewing VSD/RTO Information

Double-click the cluster security device icon or click the + icon that corresponds to the cluster security device icon to view the virtual security devices (VSD) and run-time objects (RTO) that have been attached to this cluster.

Click the VSD or RTO icon and summary information describing the object appears. The following table describes the information available from the VSD/RTO summary:

Table 52: VSD/ RTO Summary

<table>
<thead>
<tr>
<th>Item</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster</td>
<td>the name of the cluster associated with this VSD.</td>
</tr>
<tr>
<td>VSD(RTO)</td>
<td>the name of this VSD (or RTO).</td>
</tr>
<tr>
<td>No of Devices</td>
<td>the total number of security devices that are associated with this VSD.</td>
</tr>
<tr>
<td>Init Hold Time (sec)</td>
<td>the initial hold time state (in seconds) of the VSD.</td>
</tr>
<tr>
<td>Heartbeat Interval (ms)</td>
<td>the time interval (in milliseconds) between each heartbeat.</td>
</tr>
<tr>
<td>Heartbeat Lost Threshold (ms)</td>
<td>threshold level required to change over to the backup security device.</td>
</tr>
<tr>
<td>Master</td>
<td>the Master System.</td>
</tr>
<tr>
<td>Primary Backup</td>
<td>the Primary System.</td>
</tr>
</tbody>
</table>
Viewing VSD Counter Details

Click the Counters tab to view specific information about your VSD counters. The following table describes the information that is available from the VSD counters view:

Table 53: VSD Counter Details

<table>
<thead>
<tr>
<th>Item</th>
<th>Displays</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>the device(s) that are associated with the VSD (or RTO).</td>
</tr>
<tr>
<td>Number of Units</td>
<td>the number of units associated with the VSD (or RTO).</td>
</tr>
<tr>
<td>State Change Counter</td>
<td>the number of times a device changes operational states.</td>
</tr>
<tr>
<td>Init Counter</td>
<td>the transient state of a VSD (or RTO) group member while it was in the process of joining the VSD (or RTO) group.</td>
</tr>
<tr>
<td>Master</td>
<td>the number of Master devices.</td>
</tr>
<tr>
<td>Primary BackUp</td>
<td>the number of primary backup devices.</td>
</tr>
<tr>
<td>BackUp</td>
<td>the total number of backup devices.</td>
</tr>
<tr>
<td>Ineligible</td>
<td>Notes that an administrator purposefully assigned a device so that it cannot participate in the selecting a new master device.</td>
</tr>
<tr>
<td>InOperable</td>
<td>Notes that a VSD (or RTO) group device has an internal problem.</td>
</tr>
<tr>
<td>Master Conflict</td>
<td>the number of conflicts that occurred on the master device.</td>
</tr>
<tr>
<td>Primary Backup Conflict</td>
<td>the number of conflicts that occurred on the primary backups device.</td>
</tr>
<tr>
<td>Tx Heartbeat</td>
<td>the number of transmitted heartbeats on the devices.</td>
</tr>
<tr>
<td>Rx Heartbeat</td>
<td>the number of received heartbeats on the devices.</td>
</tr>
</tbody>
</table>

Viewing RTO Counter Details

Click the Counters tab to view specific information about your RTO counters. The following table describes the information that is available from the RTO counters view:

Table 54: RTO Counters Details

<table>
<thead>
<tr>
<th>Item</th>
<th>Displays</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>the device(s) that are associated with the RTO.</td>
</tr>
<tr>
<td>Member ID</td>
<td>the member identification associated with this RTO</td>
</tr>
<tr>
<td>Status</td>
<td>the current status of the RTO: Active or Down.</td>
</tr>
<tr>
<td>Direction</td>
<td>the direction of the RTO: In or Out.</td>
</tr>
<tr>
<td>Lost Heartbeat</td>
<td>the number of heartbeats not received from the RTOs peers.</td>
</tr>
<tr>
<td>Counter to Active</td>
<td>the number of times that the RTO was placed to “active”</td>
</tr>
<tr>
<td>Counter to Set</td>
<td>the number of times that the RTO was placed to “set”</td>
</tr>
<tr>
<td>Counter to Lost Peer</td>
<td>the number of times that the RTO was placed to Lost Peer.</td>
</tr>
<tr>
<td>Counter to Group Detach</td>
<td>the number of times that the RTO was placed to Group Detach.</td>
</tr>
</tbody>
</table>
Using The Realtime Monitor

The following examples describe typical use cases for monitoring your security devices, VPNs, and NSRP clusters in NetScreen-Security Manager.

EXAMPLE: MONITORING DEVICE STATUS
In this example, you are a network administrator responsible for monitoring the day-to-day operation of all the security devices managed in your network. You are using NetScreen-Security Manager to manage your network, and Realtime Monitor to monitor the up/down connection status of all your security devices.

One day, you notice that the Connection Status on a mission-critical security device indicates that the security device is DOWN. You wait several minutes to verify that the connection status doesn't resolve itself as intermittent network problems may cause a security device to temporarily indicate as DOWN. The Device Monitor still indicates that the security device is DOWN.

You next try to ping the security device. If you are successful in reaching the device, you can send a `get status` command to check the status of the security device.

If you cannot ping the security device, you will want to investigate further what may be a potential problem with the security device or your network. You next scan the Log Viewer for the log entry indicating that the security device has disconnected. You can filter the log entries in the Log Viewer to display only the log entries generated for the security device during the immediate time period that it went down. Viewing these log entries will also provide you with a context around the events leading to the security device disconnecting. This will help you to determine the cause of the problem.

You notice several very suspicious log entries that indicate that this security device may have been the target of an attack. You flag the log entries using the pre-defined flag types in the Log Viewer, and assign them to your security experts for further investigation.

Monitoring the Management System

Use the Server Manager to access, monitor, and configure the NetScreen-Security Manager management system. The management system consists of a GUI Server and Device Server. Refer to the NetScreen-Security Manager 2005.3 Installer’s Guide for more information about the GUI Server and Device Server.

Security Manager contains the following:

- Servers
- Server Monitor

Configuring Servers

Use Servers to add, configure and view key information about the GUI Server and Device Server:
### Configuring Device Servers

You can also add and configure a Device Server. You might need to configure a Device Server when installing the GUI Server and Device Server on separate servers, or when installing the management system with High Availability (HA) enabled.

You can configure the following parameters on a Device Server:

- **Name**—you can give the Device Server any name you wish
- **IP Address**—IP address of the Device Server.
- **Server Type**—either Device Server or Device Server Cluster. If you are installing the management system with HA enabled, you need to configure the Device Server as part of an HA Cluster. After you specify that a Device Server will act as a Device Server Cluster, you can access additional tabs allowing you to further configure cluster details including the IP Address and port number of the secondary server, and e-mail notification.
- **Device Server Manager Port**—the port is set to 7800 by default.
- **Device Server ID**—this is a unique ID assigned by NetScreen-Security Manager to each Device Server.
- **Mapped IP Address (if applicable)**—you can define multiple mapped IP addresses.
- **Device Polling**—the Device Server polls security devices it manages for Device, VPN, NSRP, or Interface statistics every 300 seconds by default. If you wish to change this behavior, you can edit the interval, using the Device Polling tab.
- **High Availability (HA)**—in order to configure a secondary Device Server, you need to specify the IP Address and port, and Mapped IP Address (if applicable).
- **Email Notification**—you can configure an SMTP server to send you an email notifying you of various events on the Device Server.

**NOTE:** You must restart the GUI Server to apply any changes that you have made.

Refer to the NetScreen-Security Manager Installer’s Guide for more information on adding and configuring the Device Server.

---

**Table 55: Server Information**

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the GUI Server or Device Server.</td>
</tr>
<tr>
<td>Server Type</td>
<td>whether the current server is a GUI Server, GUI Server Cluster, Device Server, or Device Server Cluster.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of the server.</td>
</tr>
<tr>
<td>Device Server Manager Port</td>
<td>the port open on the Device Server for security devices running ScreenOS 5.x.</td>
</tr>
</tbody>
</table>
Configuring the GUI Server

You can configure the following parameters for the GUI Server:

- **Server Type**—Select GUI Server or GUI Server Cluster. If you are installing the management system with HA enabled, you need to configure the GUI Server as part of an HA Cluster.
- **IP Address**
- **HA parameters**
- **Email Notification**—you can configure an SMTP server to send you an email notifying you of various events on the GUI Server.

**NOTE:** You must restart the GUI Server to apply any changes that you have made.

Using Server Monitor

You can use the Server Monitor to view the status of the running GUI Server and Device Server. The Server Monitor lists all GUI Servers and Device Servers in your management system. For example, if you have installed a primary and secondary GUI Server in a high availability configuration, you could use the Server Monitor to monitor which GUI Server is currently active.

The Server Monitor provides two categories of information:

- **Server status**—displays information about the GUI Server or Device Server's status, CPU, and memory. You can also choose to view the status of each server in the Server Monitor, or view additional server status details in a separate dialog box.
- **Process status**—displays information about the individual processes on a GUI Server or Device Server.

Viewing Server Status

To view the status of any server in the management system, select Server Manager in the navigation tree, and then select Server Monitor, as shown below:

![Server Monitor](image)

The following table lists and describes the columns that appear in the Server Monitor:

<table>
<thead>
<tr>
<th>Name</th>
<th>Server Type</th>
<th>Status</th>
<th>CPU</th>
<th>Mem</th>
<th>CPU Usage</th>
<th>Peer Device Server State</th>
</tr>
</thead>
<tbody>
<tr>
<td>server_1</td>
<td>Device Server</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
<td>4%</td>
<td>N/A</td>
</tr>
</tbody>
</table>
### Table 56: Server Monitor Data

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the GUI Server or Device Server.</td>
</tr>
<tr>
<td>Server Type</td>
<td>whether the current server is a GUI Server, GUI Server Cluster, Device Server, or Device Server Cluster.</td>
</tr>
</tbody>
</table>
| Status             | Status of the server based on CPU or Memory utilization:  
|                    | - OK  
|                    | - Warning  
|                    | - Critical  
|                    | - Down  
| CPU                | Status based on CPU utilization:  
|                    | - OK (CPU usage < 90%)  
|                    | - Warning (CPU usage = 90-95%)  
|                    | - Critical (CPU usage > 95%)  
|                    | - N/A (when the server is down)  
| Mem                | Displays status based on memory utilization:  
|                    | - OK (memory usage < 99%)  
|                    | - Warning (memory usage > 99%)  
|                    | - Critical (memory usage = 100%)  
|                    | - N/A (when the server is down)  
| CPU Usage          | Percentage of CPU used. |
| Peer Device Server State | Displays the state of the server's peer server (only applicable if you have added a secondary server and configured it in an HA Cluster). |
| Active Server      | Displays whether the currently active server is the primary or secondary server in an HA Cluster. |
| Last GUI Server Replication Time | Time of day that the GUI Server database was last replicated to its peer server. |

You can sort data in the Server Monitor according to any column header by simply clicking that column.

### Viewing Additional Server Status Details

If you are interested in monitoring additional details about your server's status, you can view the Server Detail Status window by double-clicking any of the servers that appear in the Server Monitor. You can also right-click anywhere on the Server Monitor and select View Details. The Server Detail Status dialog box appears.
The following table describes information available in the Server Detail Status:

Table 57: Server Detail Status

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS</td>
<td>Operating system running on server machine.</td>
</tr>
<tr>
<td>Type</td>
<td>The server’s machine processor type.</td>
</tr>
<tr>
<td>CPU Idle</td>
<td>Percentage of the time the CPU was idle.</td>
</tr>
<tr>
<td>CPU User</td>
<td>Percentage of CPU utilization that occurred while executing at the user level.</td>
</tr>
<tr>
<td>CPU Kernel</td>
<td>Percentage of CPU utilization that occurred while executing at the system level.</td>
</tr>
<tr>
<td>CPU Usage</td>
<td>Percentage of CPU utilization.</td>
</tr>
<tr>
<td>1 Min Load</td>
<td>One minute load average.</td>
</tr>
<tr>
<td>5 Min Load</td>
<td>Five minute load average.</td>
</tr>
<tr>
<td>15 Min Load</td>
<td>Fifteen minute load average.</td>
</tr>
<tr>
<td>Total Mem</td>
<td>Total amount (in megabytes or gigabytes) of memory.</td>
</tr>
<tr>
<td>Used Mem</td>
<td>Amount (in megabytes or gigabytes) of used memory.</td>
</tr>
</tbody>
</table>
Viewing Process Status

From the Server Monitor, you can also view the status of all running server processes on the GUI Server or Device Server. This view is useful for troubleshooting purposes. If you are having problems with the server, you can quickly identify if a specific process on the server is the source of that problem.

To view process status, select Server Manager in the navigation tree, and then select Server Monitor. Double click the Server Monitor or click the node to expand the navigation tree. You can also right-click the Server Monitor to open it in a new window. Click to select a server to view the status of the processes running on it.

The following graphic depicts process status for the Device Server.

Figure 194: Process Status for the Device Server

<table>
<thead>
<tr>
<th>Name</th>
<th>Status</th>
<th>Total Mem Used</th>
<th>Phys. Mem Used</th>
<th>CPU Usage</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>.devSvrDataCollector</td>
<td>Up</td>
<td>670 MB</td>
<td>19 MB</td>
<td>0%</td>
<td>Version NSM 2</td>
</tr>
<tr>
<td>.devSvrDirectiveHandler</td>
<td>Up</td>
<td>691 MB</td>
<td>8 MB</td>
<td>0%</td>
<td>Version NSM 2</td>
</tr>
<tr>
<td>.devSvrLogWalker</td>
<td>Up</td>
<td>6 MB</td>
<td>3 MB</td>
<td>0%</td>
<td>v1.3.1 (build LG)</td>
</tr>
<tr>
<td>.devSvrManager</td>
<td>Up</td>
<td>16 MB</td>
<td>4 MB</td>
<td>0%</td>
<td>v1.3.1 (build LG)</td>
</tr>
<tr>
<td>.devSvrStatusMonitor</td>
<td>Up</td>
<td>5 MB</td>
<td>3 MB</td>
<td>2%</td>
<td>v1.3.1 (build LG)</td>
</tr>
</tbody>
</table>

The following figure depicts process status for the GUI Server.

Figure 195: Process Status for the GUI Server

<table>
<thead>
<tr>
<th>Name</th>
<th>Status</th>
<th>Total Mem Used</th>
<th>Phys. Mem Used</th>
<th>CPU Usage</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>.guiSvrDirectiveHandler</td>
<td>Up</td>
<td>650 MB</td>
<td>15 MB</td>
<td>0%</td>
<td>Version NSM 20</td>
</tr>
<tr>
<td>.guiSvrManager</td>
<td>Up</td>
<td>58 MB</td>
<td>46 MB</td>
<td>0%</td>
<td>v1.3.1 (build LG)</td>
</tr>
<tr>
<td>.guiSvrMasterController</td>
<td>Up</td>
<td>649 MB</td>
<td>7 MB</td>
<td>0%</td>
<td>Version NSM 20</td>
</tr>
<tr>
<td>.guiSvrStatusMonitor</td>
<td>Up</td>
<td>5 MB</td>
<td>3 MB</td>
<td>2%</td>
<td>v1.3.1 (build LG)</td>
</tr>
</tbody>
</table>

The following table lists and describes the information that appears in the Process Status:
Table 58: Process Status

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the GUI Server or Device Server process.</td>
</tr>
<tr>
<td>Status</td>
<td>Displays if the process is Up or Down.</td>
</tr>
<tr>
<td>Total Mem Used</td>
<td>Total amount (in megabytes) of memory utilized.</td>
</tr>
<tr>
<td>Phys Mem Used</td>
<td>Total amount (in megabytes) of physical memory utilized.</td>
</tr>
<tr>
<td>CPU Usage</td>
<td>Percentage of CPU utilized.</td>
</tr>
<tr>
<td>Version</td>
<td>Process version.</td>
</tr>
</tbody>
</table>

You can sort server monitor data according to any column header by clicking that column.
Juniper Networks NetScreen-Security Manager integrates log information from multiple devices into a seamless environment to help you easily access and distill data about the traffic on your network.

The Log Viewer presents log data as a log entry in a table; a log entry contains the details of the traffic that triggered the log, such as IP address, port number, and source and destination zones. This log data is also automatically used to generate predefined Reports, helping you interpret event information in a specific context. Or, to perform your own investigation, use the Log Investigator to view cross-tabulations between sources, destinations, subcategories, and destination ports.

The Audit Log Viewer presents log entries triggered by administrative changes (changes made to the NetScreen-Security Manager system). An audit log entry includes details about the administrative event, such as the administrator name, timestamp of the change, and job details.

You can configure each managed security device to generate and export specific log records to multiple formats and locations, such as syslog, xml, or email servers. You can also forward logs that meet specified criteria to predefined formats and locations.

The following sections are in this chapter:

- About Logging
- Configuring Logging
- Using the Log Viewer
- Using the Log Investigator
- Using the Audit Log Viewer
- Managing Log Volume
- Forwarding Logs
About Logging

Logging is the act of recording information about an event. In NetScreen-Security Manager, each event that occurs on your network or in your management system can be recorded and stored as a log entry. To view log entries from the Juniper Networks NetScreen-Security Manager UI, you can use one or more of the logging-related UI components, such as the Log Viewer or the Log Investigator.

It may be helpful to visualize log entries being sent or pushed from the device to the Juniper Networks NetScreen-Security Manager Device Server, which then pushes the log entries to the logging database. A UI module (the Log Viewer or Report Manager) requests or pulls the log entries in the logging database and displays the entries in the UI.

About Log Entries

A managed device generates a log entry when an event matches the configured logging conditions. The log entry, which contains details of the event, is sent to the NetScreen-Security Manager Device Server and stored in the logging database. You can view log entries in the NetScreen-Security Manager UI.

In a single log entry, you can view detailed information about where traffic comes from (the source address), where traffic goes (the destination address) and a description of the event that triggered the log entry. You can also view summarized information about events and alarms for multiple log entries. This data can help you analyze log entries and determine the effectiveness of your current Security Policies and device configurations.

About Log Events

Managed devices generate log entries based on events. Typically, devices generate log entries when:

- An event matches a rule in which logging is enabled. When you configure a rule for logging, the device creates a log entries for each event that matches that rule.

- An event matches a predefined set of conditions configured on a managed device or the management system.

Some events generate log entries that appear in the Log Viewer, while others appear in RealTime Monitor. The following table details event-generated log entries:
Table 59: Event-Generated Log Entries

<table>
<thead>
<tr>
<th>Events</th>
<th>Description</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack, Alarm, Other</td>
<td>Generates log entries for events related to network activity on the device that violates a set threshold.</td>
<td>Log Viewer</td>
</tr>
<tr>
<td>VPN Events</td>
<td>Generates log entries for events related to VPN tunnels. These log entries are used to produce statistical information for monitoring purposes.</td>
<td>Realtime Monitor &gt; VPN Monitor</td>
</tr>
<tr>
<td>Configuration, Information, Self, Policy, Traffic</td>
<td>Generates log entries for events related to device configuration, NetScreen-Security Manager configuration, Security Policy rules, and traffic activity on the managed device.</td>
<td>Log Viewer</td>
</tr>
<tr>
<td>Flow, Ethernet, Attack, Policy</td>
<td>Generates log entries for events related to packet flow, ethernet objects, network attacks, and Security Policy rules. These log entries are used to produce statistical information for monitoring purposes.</td>
<td>Realtime Monitor &gt; Device Monitor</td>
</tr>
<tr>
<td>Protocol Distribution</td>
<td>Generates log entries for events related to protocols used in network activity. These log entries are used to produce statistical information for monitoring purposes.</td>
<td>Realtime Monitor &gt; Device Monitor</td>
</tr>
</tbody>
</table>

Table 60: Log Categories

<table>
<thead>
<tr>
<th>Log Type</th>
<th>Generated When</th>
<th>Configured In</th>
</tr>
</thead>
<tbody>
<tr>
<td>Predefined</td>
<td>Traffic matches a signature or protocol anomaly attack group.</td>
<td>Device Configuration &gt; Report Settings &gt; NSM Security Policies &gt; Rule Options &gt; Attack Protection</td>
</tr>
<tr>
<td>Config</td>
<td>A configuration or operational state changed in NetScreen-Security Manager.</td>
<td>Device Configuration &gt; Report Settings &gt; NSM</td>
</tr>
<tr>
<td>Custom</td>
<td>Traffic matches a Custom Attack Object.</td>
<td>Security Policies &gt; Rule Options &gt; Attack Protection</td>
</tr>
<tr>
<td>Info</td>
<td>Details general system information.</td>
<td>Device Configuration &gt; Report Settings &gt; NSM</td>
</tr>
<tr>
<td>Self</td>
<td>A non traffic-related event occurs.</td>
<td>Device Configuration &gt; Report Settings &gt; General</td>
</tr>
<tr>
<td>Screen</td>
<td>Traffic matches a Screen-level attack.</td>
<td>Device Configuration &gt; Network &gt; Zone</td>
</tr>
</tbody>
</table>
About Log Severity

The log severity level defines the urgency of the information contained in the log entry. The severity level of a log entry depends on the log category, such as information, traffic, or configuration log entries.

You can configure a managed device to generate log entries only for those events that meet a specific severity level criteria. Additionally, you can configure the device to forward log entries that contain a specific severity to a specific destination, such as a console location or syslog server. You can forward multiple log entries with different severity levels to the same log destination.

Juniper Networks assigns a predefined severity level in the firmware of each Juniper Networks security device. However, these severity levels are not the same as the severity levels that appear in the log entries viewed in a NetScreen-Security Manager UI module.

The following table details how NetScreen-Security Manager handles Juniper Networks ScreenOS severity levels:

Table 61: Log Entry Severities

<table>
<thead>
<tr>
<th>NetScreen-Security Manager Severity</th>
<th>ScreenOS Severity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>Emergency</td>
<td>Log entries triggered when traffic matches a critical severity attack object. Also includes log entries triggered by the SCREEN level attacks SYN attacks, Tear Drop attacks, and Ping of Death attacks.</td>
</tr>
<tr>
<td>Alert</td>
<td></td>
<td>Log entries triggered by the general firewall SCREEN level attacks or other conditions that require immediate attention, such as the expiration of license keys.</td>
</tr>
<tr>
<td>Major</td>
<td>Critical</td>
<td>Log entries triggered when traffic matches a major severity attack object. Also includes log entries triggered by changes in the device functionality, such as high availability (HA) status changes.</td>
</tr>
<tr>
<td>Minor</td>
<td>Error</td>
<td>Log entries triggered when traffic matches a minor severity attack object. Also includes log entries triggered by errors in device functionality, such as a failure in antivirus scanning or in communicating with SSH servers.</td>
</tr>
<tr>
<td>Warning</td>
<td>Warning</td>
<td>Log entries triggered when traffic matches a warning severity attack object. Also includes log entries triggered by questionable device activity, such as a failure to connect to email servers and authentication failures, timeouts, and successes.</td>
</tr>
</tbody>
</table>
Configuring Logging

Before your managed device can generate log entries or log data, you must configure your devices and the NetScreen-Security Manager system for logging. You can configure an individual device to generate attack, alarm, configuration, information, and self log entries for specific destinations.
To view log entries and log data in the NetScreen-Security Manager UI, you must configure the individual device to generate log information for NetScreen-Security Manager, and enable one or more severity settings for NetScreen-Security Manager. However, you are not required to configure the settings for other destinations if you do not use those destinations for log management.

**Configuring the Device for Logging**

At the device level, you can configure how and where the device sends its log entries. For each destination, you can define:

- The category of log entries you want the device to generate and forward to a specific destination, and
- The severity of log entries you want the device to forward to a specific destination

The severity setting applies to all log types for that destination. For example, if traffic log entries are enabled for NetScreen-Security Manager, but the severity setting specifies critical and major severities, NetScreen-Security Manager receives only critical and major traffic logs; all other severity traffic log entries are generated, but never sent to the management system. Unsent traffic log entries are stored on the device and discarded when the device log storage capacity is exceeded.

**Configuring Severity Settings**

Use the General settings to select the severity levels of the log entries you want to forward to a specific location. Juniper Networks assigns a predefined severity level for each event that generates a log entry on a security device; using NetScreen-Security Manager, you can configure a device to send log entries with specific severity levels to specific destinations.

For each destination (except Firewall Options), you can specify one or more severity levels (for details on severity levels, see “About Log Severity” on page 722).

---

**NOTE:** Debug messages are sent only to syslog, and do not appear in any NetScreen-Security Manager UI module.

---

Not all destinations support all log entry severities. The following table details the log entry severities accepted by each destination (except Firewall Options):
Table 62: Destinations of Log Entry Severities

<table>
<thead>
<tr>
<th>Destination</th>
<th>Description</th>
<th>Severities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console</td>
<td>The PC you use to view log entries in NetScreen-Security Manager.</td>
<td>All severities</td>
</tr>
<tr>
<td>Email</td>
<td>An Email server to which you want log information forwarded.</td>
<td>Emergency, Alert, Critical, Notification</td>
</tr>
<tr>
<td>Syslog</td>
<td>The syslog facility on the Device Server.</td>
<td>All severities</td>
</tr>
<tr>
<td>WebTrends</td>
<td>A WebTrends server to which you want log entries forwarded.</td>
<td>All severities</td>
</tr>
<tr>
<td>NetScreen-Security Manager</td>
<td>The NetScreen-Security Manager server.</td>
<td>All severities</td>
</tr>
<tr>
<td>PCMCIA</td>
<td>A PCMCIA device to which you want log entries forwarded.</td>
<td>All severities</td>
</tr>
<tr>
<td>Internal</td>
<td>An destination within the current device to which you want log entries forwarded.</td>
<td>All severities</td>
</tr>
</tbody>
</table>

To select log entry severities for a destination, open a device configuration and select Report Settings > General, then select the destination.

**Forwarding Self Log Entries (Firewall Options)**

Self log entries display information on traffic that was dropped by the security device or on traffic that terminates on the device. Any packet that terminates at the device generates a self log entry; Telnet, Ping, BGP, and OSPF connections all terminate at the device, and can trigger a self log entry.

A self log includes the date and time a packet was dropped, the source address of the packet, the destination address of the packet, the duration for which the packet was active, and the service associated with the packet. You can disable or enable logging of dropped packets for specific traffic types, including ICMP, IKE, SNMP, and multicast packets.

To configure self log entries, open a device configuration and select Report Settings > General. Click the Firewall Options tab and configure the following settings:
Table 63: Self Log Entry Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log ICMP Packets to Self</td>
<td>Creates a log entry for an ICMP (ping) packet that was dropped or terminated at the device.</td>
</tr>
<tr>
<td>Log IKE Packets to Self</td>
<td>Creates a log entry for an IKE packet that was dropped or terminated at the device. When negotiating an IKE key, the VPN client communicates with the security device.</td>
</tr>
<tr>
<td>Log SNMP Packets to Self</td>
<td>Creates a log entry for an SNMP packet that was dropped or terminated at the device.</td>
</tr>
<tr>
<td>Log Multicast Packets to Self</td>
<td>Creates a log entry for a multicast packet that was dropped or terminated at the device.</td>
</tr>
</tbody>
</table>

Configuring Email Server Settings

Use the Email option to configure a security device to send messages using email whenever a system event of Emergency, Alert, Critical, or Notification severity level occurs. You can configure the email and SMTP settings at the device level, or skip this section and configure the GUI server to handle emails; see “Exporting to Email” on page 771.

To configure email server settings and enable the device to send email messages, open a device configuration and select Report Settings > Email. Configure the following settings:

Table 64: Email Server Settings for Log Entries

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Notification for Alarms</td>
<td>When alarm is enabled for a rule in the installed Security Policy and traffic matches the rule, the device sends an email notification to the specified SMTP server.</td>
</tr>
<tr>
<td>Include Traffic Log</td>
<td>When logging is enabled for a rule in the installed Security Policy and traffic matches the rule, the device sends the traffic log entry to the specified SMTP server.</td>
</tr>
<tr>
<td>SMTP Server Name</td>
<td>The name of the Simple Mail Transfer Protocol server that receives email notification messages. You must specify the SMTP server name and at least one email address to receive email notification.</td>
</tr>
<tr>
<td>Email Address 1</td>
<td>The primary email address that receives email notification messages from the device.</td>
</tr>
<tr>
<td>Email Address 2</td>
<td>The secondary email address that also receives email notification from the device.</td>
</tr>
</tbody>
</table>

Configuring Events Reporting Settings

Use the Events reporting settings to configure the security device to report specific events to NetScreen-Security Manager.
Select the appropriate NetScreen-Security Manager Device Server, then select the events that are logged on the security device and reported to NetScreen-Security Manager. The following sections detail each event.

NOTE: For security devices running ScreenOS 4.0.x, you must also select Enable Logging.

**Screen Alarm Log Entries**

The device generates screen alarm log entries when a security device detects network traffic that matches the screen settings enabled on the device.

To receive screen alarm log entries, you must:

- Enable the device to generate screen alarm log entries for NetScreen-Security Manager in Report Settings > NSM.
- Enable the device to send log entries with the desired severity settings to NetScreen-Security Manager in Report Settings > General > NSM.
- Enable screen attack protection on the device. For details, see “Configuring SCREEN Attack Protection” on page 213.

Screen alarm log entries appear in the Log Viewer and display the following columns of information in the Log Viewer:

- Source Address
- Destination Address
- Service
- Action
- Category (Screen)
- Subcategory (for details on Screen subcategories, see “Screen Alarm Log Entries” on page 832)
- Severity

**Event Alarm Log Entries**

The device generates event alarms for any security event that has a predefined severity level of emergency, critical, or alert. Event alarms generate log entries that appear in the Alarm category.

To receive event alarm log entries, you must:

- Enable the device to generate event alarm log entries for NetScreen-Security Manager in Report Settings > NSM.
- Enable the device to send log entries with emergency, alert, and critical severity settings to NetScreen-Security Manager.
Event alarms appear in the Log Viewer under the Alarm category. For details on Attack subcategories, see “Alarm Log Entries” on page 833.

**Traffic Alarm Log Entries**
The device generates traffic alarm log entries when your security device detects network traffic that exceeds the specified alarm threshold in a Security Policy rule. The traffic alarm log entry, which displays in the Log Viewer, describes the security event that triggered the alarm. Traffic alarms generate log entries that appear in the Alarm category.

To receive traffic alarm log entries, you must:

- Enable the device to generate traffic alarm log entries for NetScreen-Security Manager in Report Settings > NSM.
- Enable the device to send log entries with the desired severity settings to NetScreen-Security Manager.
- Enable counting and alarms in the Security Policy installed on the device. For details on configuring traffic alarm logging in your Security Policy rules, see “Configuring Counting and Alarms” on page 545.

Traffic alarms appear in the Log Viewer under the Alarm category. For details on alarm subcategories, see “Alarm Log Entries” on page 833.

Alarm log entries contain information in the following Log Viewer columns:

- To Zone
- From Zone
- Source IP
- Destination IP
- Threshold (displayed in the Misc. column of the Log Viewer)

**Deep Inspection Alarm Log Entries**
The device generates Deep Inspection alarm log entries when a security device with Deep Inspection (DI) detects network traffic that matches an attack object specified in a Security Policy rule. When matched in a rule, protocol anomaly attack objects, signature attack objects, and custom attack objects all generate Deep Inspection alarm log entries that appear in the Log Viewer.

To receive Deep Inspection alarm log entries, you must:

- Enable the device to generate Deep Inspection alarm log entries for NetScreen-Security Manager in Report Settings > NSM.
- Enable the device to send log entries with the desired severity settings to NetScreen-Security Manager in Report Settings > General > NSM.
Enable Deep Inspection detection in the Security Policy installed on the device. For details on configuring Deep Inspection logging in your Security Policy rules, see “Configuring a DI Profile/Enable IDP For Firewall Rules” on page 551.

Deep Inspection alarm log entries appear in the Log Viewer and display the following columns of information in the Log Viewer:

- Source Address
- Destination Address
- Service
- Action
- Category (Predefined or Custom)
- Subcategory (for details on Deep Inspection alarm subcategories, see “Deep Inspection Alarm Log Entries” on page 834)
- Severity

### Configuration Log Entries

The device generates configuration log entries for events that change the configuration on the device. Specifically, any command issued that the ScreenOS get config command statement captures and displays in ScreenOS generates a configuration log. For each configuration change, the device generates a configuration log entry that contains information about the change in the Log Viewer Detail column.

To receive configuration log entries, you must:

- Enable the device to generate configuration log entries for NetScreen-Security Manager in Report Settings > NSM.
- Enable the device to send log entries with a notification severity setting to NetScreen-Security Manager in Report Settings > General > NSM.

Configuration log entries appear in the Log Viewer under the category Configuration. For details on configuration subcategories, see “Configuration Log Entries” on page 898.

### Information Log Entries

The device generates information logs when it detects that an administrator has made a change to the basic settings of the device, such as logging in/log out, setting a new password for the device, issuing a key value for the device, or entering an MD5 authentication password to enter a device. For each administrative change, the device generates an information log entry that contains information about the change in the Log Viewer Detail column.

To receive information log entries, you must:
Enable the device to generate information log entries for NetScreen-Security Manager in Report Settings > NSM.

Enable the device to send log entries with the info, warning, and error severity settings to NetScreen-Security Manager in Report Settings > General > NSM.

Information log entries appear in the Log Viewer under the category Information. For details on information subcategories, see “Information Log Entries” on page 900.

Self Log Entries
The device generates self log entries for any packet that terminates at the device. Self log entries display information on traffic that was dropped by the security device or on traffic that terminates on the device.

To receive self log entries, you must:

Enable the device to generate self log entries for NetScreen-Security Manager in Report Settings > NSM.

Enable the device to send specific self log entries to NetScreen-Security Manager in Report Settings > General > Firewall Options. For details, see “Forwarding Self Log Entries (Firewall Options)” on page 725.

Self log entries appear in the Log Viewer under the category Self, which contains information in the following Log Viewer columns:

- Source
- Destination
- Services

Self log entries have the category “Self” and the subcategory “Self Log”.

Traffic Log Entries
The device generates traffic log entries when your security device detects network traffic that matches the source, destination, and service specified in a Security Policy rule.

To receive traffic log entries, you must:

Enable the device to generate traffic log entries for NetScreen-Security Manager in Report Settings > NSM.

Enable the device to send log entries with the desired severity settings to NetScreen-Security Manager.

Enable logging in the Security Policy installed on the device. For details on configuring traffic logging in your Security Policy rules, see “Configuring Logging and Alerts” on page 545.
Traffic log entries appear in the Log Viewer under the Traffic category. For details on
traffic subcategories, see “Traffic Log Entries” on page 901.

Policy Statistics
The device forwards statistics on the policy distribution of the traffic that entered
the device. Policy distribution statistics do not generate log entries; the information
is used by the Realtime Monitor module. For details on how policy distribution
appears in Realtime Monitor, see “Viewing Traffic Distribution by Security Policy”
on page 690.

Attack Statistics
The device forwards statistics for attacks detected in the traffic that entered the
device. Attack statistics do not generate log entries; the statistics are used by the
Realtime Monitor module. For details on how attack statistics appear in Realtime
Monitor, see “Viewing Attack Statistics” on page 699.

Ethernet Statistics
The device forwards statistics for ethernet activity on the device. Ethernet statistics
do not generate log entries; the statistics are used by the Realtime Monitor module.
For details on how ethernet statistics appear in Realtime Monitor, see “Viewing
Ethernet Statistics” on page 697.

Flow Statistics
The device forwards statistics for flows that entered the device. Flow statistics do
not generate log entries; the statistics are used by the Realtime Monitor module. For
details on how flow statistics appear in Realtime Monitor, see “Viewing Flow
Statistics” on page 699.

Protocol Distribution
The device forwards information on the protocol distribution of the traffic that
entered the device. Protocol distribution information does not generate log entries;
the information is used by the Realtime Monitor module. For details on how
protocol distribution appears in Realtime Monitor, see “Viewing Traffic Distribution
by Protocol” on page 693.

The device reports statistics generated by the following services:

- AH (Authentication Header)
- ESP (Encapsulating Security Payload)
- GRE (Generic Routing Encapsulation)
- ICMP (Internet Control Message Protocol)
- OSPF (Open Shortest Path First)
- TCP (Transmission Control Protocol)
- UDP (User Datagram Protocol)
You can also set the interval at which the NetScreen-Security Manager Device Server polls for policy statistics and protocol distribution events.

**Atomic Updating Events**

Devices running ScreenOS 5.1 or higher support atomic updating, which enables the device to receive the entire modeled configuration (all commands) before executing those commands (instead of executing commands as they are received from the management system). Atomic updating also enables the device to temporarily lose connection to NetScreen-Security Manager during the update process.

If the device cannot reconnect to the management system after processing the update, it automatically reboots (with the previously saved configuration) and reconnects to the management system. To prevent a device from rebooting and/or configure the reboot timeout, open a device configuration and select Report Settings > Events, then configure the Atomic Updating options.

For details on Atomic Updating, see “About Atomic Updating (ScreenOS 5.1 or Higher Only)” on page 392.

**Configuring SNMP Reporting Settings**

Use SNMP settings to configure the Simple Network Management Protocol (SNMP) agent for the security device. The SNMP agent provides a view of statistical data about the network and the devices on it, and notification of system events of interest. You can configure the SNMP settings at the device level, or skip this section and configure the GUI server to handle SNMP reporting; see “Exporting to SNMP” on page 770.

In addition to configuring the SNMP reporting settings, you also must enable SNMP management service options on the interface through which the SNMP manager application communicates with the SNMP agent in the security device. For details on enabling management service options, “Configuring Interface Service Options” on page 226.

To configure SNMP settings and enable the device to send SNMP traps, open a device configuration and select Report Settings > SNMP. Configure the following settings:

- **System Name**—The name of the device for which you are generating SNMP status.

- **Contact Person**—The name of the network administrator who manages the device. This contact information is useful when the SNMP community member needs to contact someone about the device.

- **Location**—The physical location of the device.

- **Listen Port**—The number of the port assigned to monitor SNMP traffic (listen and transmit SNMP traps).

- **Trap Port**—The number of the port assigned to transmit traps that have been generated by an SNMP alarm, threshold violation, or error.
Enable Authentication Fail Trap—Specifies whether you want to generate a trap if a packet fails to be authenticated when attempting to enter the device. Select this option if the device sends SNMP messages through a VPN tunnel.

Next, configure SNMP communities. To send traps, the SNMP agent on the security device requires that you define communities, their associated hosts, and assign permissions (read/write or read-only). You can create up to three (3) SNMP communities, with up to eight (8) hosts in each community.

To create an SNMP community, click the Add icon under Community Settings and configure the following settings:

- **Community name**—The device uses the community name to authorize users attempting to enter the device.
- **Access Mode**—Defines read-write or read-only privileges for the community.
- **Traffic**—When enabled, the device can accept traffic from the source interface.
- **Version**—Defines the versions supported by the community (SNMPv1, SNMPv2c, or both SNMP versions, as required by the SNMP management stations). For backward compatibility with earlier ScreenOS releases that only support SNMPv1, security devices support SNMPv1 by default.
- **Hosts**—Define the host(s) associated with the community. Click the Add icon, then specify the host IP address and netmask, the trap version for the host (if an SNMP community supports both SNMPv1 and SNMPv2c, you must specify a trap version for each community member), and the source interface.

Directing Logs to a Syslog Server

A security device can generate syslog messages for system events at predefined severity levels and optionally for traffic that policies permit across a firewall. It sends these messages via UDP (port 514) to up to four designated syslog hosts running on UNIX/Linux systems. When you enable syslog reporting, you also specify which interface the security devices is to use to send syslog packets.

You can configure the syslog server settings at the device level, or skip this section and configure the GUI server to handle syslog messages; see “Exporting to Syslog” on page 770.

To send log entries to a Syslog server, click the Syslog option. NetScreen-Security Manager displays the Syslog dialog box. Enter appropriate data into the following fields.
Using the Log Viewer

The Log Viewer displays log entries generated by a security device when traffic matches a firewall or VPN rule, or when an event occurs that matches a predefined set of conditions. The main display of the Log Viewer displays summarized information about security events and alarms, while the detail panes provide more detailed information about a specific log entry.

This section provides details on the following Log Viewer functionality:

- About the Log Viewer UI—This section describes the Log Viewer main display area, which includes a log entry list, three detail panes, a log timeline (used for log entry navigation), and a status bar that summarizes active filters.
Searching Log Entries—For networks that generate large numbers of log entries, it can be difficult to locate the exact log entries that detail the events you want to investigate. This section describes how to use the log timeline to find logs generated around a specific time, how to use the find utility to locate log entries with a specific value, and how to search by LogID to jump directly to a specific log entry.

Filtering Log Entries by Event and Time—This section describes how to create custom filters based on event data or time. You can apply these filters to a Log Viewer column or cell to reduce the number of log entries that appear in the main display area, helping you to focus your investigations on a specific group of log entries.

Filtering Log Entries by Range—This section describes how to create custom filters based on a user-defined range. You can apply these filters to a Log Viewer column or cell to reduce the number of log entries that appear in the main display area, helping you to focus your investigations on a specific group of log entries.

Customizing Columns—The Log Viewer includes 40 columns of log entry information; however, each predefined view includes only a small subset (16) of available columns. This section describes how to set viewable columns, change column display order, resize columns, and hide/unhide a specific column.

Using Log Views—The Log Viewer includes several predefined views for critical severity attacks, configuration log entries, scans, and other important activity. This section describes how to use filters to create your own unique, customized log entry view, then save the custom view (with all its filters) for future use.

Using Log Viewer Integration—This section describes how to use the Log Viewer integration to jump from a log entry directly to the responsible Security Policy or managed device configuration.

Identifying Irrelevant Attacks—Irrelevant attacks are events that do not affect your network or that you do not consider important. For example, if you do not run an Apache Web server on your network, you do not need to worry about attacks against Apache Web servers. This section describes how to use your log entries to identify irrelevant attacks, then eliminate the attack object group that generated that attack from your Security Policy.

About the Log Viewer UI

The Log Viewer contains the following components, as shown below.
Figure 196: Log Viewer UI Overview

The Log Viewer contains the following columns:

Table 67: Log Viewer Columns

<table>
<thead>
<tr>
<th>Column</th>
<th>Default</th>
<th>What it means</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flag</td>
<td>–</td>
<td>Indicates a severity level or information type associated with the log entry. An icon used to identify a log entry. Flags are helpful for locating log entries when the Log Viewer receives large amounts of log entries. Viewer tags entries by level of severity or information type using available flag types.</td>
</tr>
<tr>
<td>Alarm</td>
<td>–</td>
<td>Indicates if an alarm has been generated with the log entry. When you configure a policy and you specify a notification for logging, you can configure an alarm to be generated when the policy performs an action.</td>
</tr>
<tr>
<td>Time Received</td>
<td>–</td>
<td>Indicates the date and the time that the Log Viewer received the log entry.</td>
</tr>
<tr>
<td>Column</td>
<td>Default</td>
<td>What it means</td>
</tr>
<tr>
<td>----------------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Source Zone</td>
<td></td>
<td>Source zone associated with a traffic log entry. Note: Log entry data for this column only appears after you update the security device. The source zone is the zone that is attempting to send the traffic through the security device.</td>
</tr>
<tr>
<td>Source Address</td>
<td>--</td>
<td>Indicates the address of the source device that generated the packet that generated the log.</td>
</tr>
<tr>
<td>Src Port</td>
<td>Default</td>
<td>Indicates the TCP/UDP port number of the source device that generated the packet that generated the log.</td>
</tr>
<tr>
<td>Destination Address</td>
<td></td>
<td>Destination zone associated with a traffic log entry. Log entry data for this column only appears after you update the security device.</td>
</tr>
<tr>
<td>Destination Address Default</td>
<td></td>
<td>Indicates the destination device to which the packet associated with the log entry was targeted.</td>
</tr>
<tr>
<td>Dst Port</td>
<td>Default</td>
<td>Indicates the TCP/UDP port number on the device to which the packet associated with the log entry was targeted.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Default</td>
<td>The connection type or protocol of the matching traffic. Protocols also have one or more port numbers.</td>
</tr>
<tr>
<td>Device Address</td>
<td>--</td>
<td>Indicates the address of the server.</td>
</tr>
<tr>
<td>Comment</td>
<td>Default</td>
<td>Enables you to add a comment that relates to the generated log entry. To enter a comment, simply click in the cell and begin typing.</td>
</tr>
<tr>
<td>Category</td>
<td>Default</td>
<td>Indicates what type of log you are viewing. Can be expressed either as a category or a sub-category. A category is either an alarm, config, misc, or traffic. A sub-category is an attack type.</td>
</tr>
<tr>
<td>Sub Category</td>
<td>Default</td>
<td>Indicates the subcategory of the log you are viewing.</td>
</tr>
<tr>
<td>Packet Data</td>
<td>--</td>
<td>Indicates the traffic type designated as part of the log entry. This indication is used to identify a packet entry created in the rulebase.</td>
</tr>
<tr>
<td>Severity</td>
<td>Default</td>
<td>Indicates the level of severity associated with the attack detected. Every attack has a default severity level although you can configure a different one.</td>
</tr>
<tr>
<td>Log ID</td>
<td>--</td>
<td>Indicates the unique identifier ID for the log entry. The log ID comprises both a date and an incrementing integer.</td>
</tr>
<tr>
<td>Action</td>
<td>--</td>
<td>Indicates whether an action occurred in response to the event that generated the log.</td>
</tr>
<tr>
<td>Alert</td>
<td>--</td>
<td>Indicates whether an alert flag was generated in response to the event that generated the log.</td>
</tr>
<tr>
<td>App</td>
<td>--</td>
<td>Indicates the application associated with the current log.</td>
</tr>
<tr>
<td>Bytes In</td>
<td>--</td>
<td>Indicates the number of bytes that comprised the log data entering the Log Viewer.</td>
</tr>
<tr>
<td>Bytes Out</td>
<td>--</td>
<td>Indicates the number of bytes that comprised the log data being transmitted from the Log Viewer.</td>
</tr>
<tr>
<td>Bytes Total</td>
<td>--</td>
<td>The sum of the number of bytes transmitted and received by the Log Viewer.</td>
</tr>
<tr>
<td>Device</td>
<td>--</td>
<td>Indicates the IP address of the device that generated the current log.</td>
</tr>
<tr>
<td>Column</td>
<td>Default</td>
<td>What it means</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------</td>
<td>---------------</td>
</tr>
<tr>
<td>Device Domain</td>
<td>--</td>
<td>Indicates the name of the domain in which the device resides.</td>
</tr>
<tr>
<td>Note: The Log Viewer displays log entries for a single domain at a time. By default, when logged in as the super admin, the Log Viewer displays log entries for managed devices in the global domain. To change the domain, apply a domain filter to view log entries for managed devices in a specific domain.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Domain Ver</td>
<td>--</td>
<td>Indicates the version number of the device.</td>
</tr>
<tr>
<td>Elapsed Secs</td>
<td>--</td>
<td>The number of seconds that have elapsed since the beginning of the current session.</td>
</tr>
<tr>
<td>From External</td>
<td>--</td>
<td>Specifies if the packet that generated this log came from an untrusted network.</td>
</tr>
<tr>
<td>Has Log Action</td>
<td>--</td>
<td>Indicates the action the device performed on the packet or connection that generated the log, generally either a permit or denial of the packet into the device.</td>
</tr>
<tr>
<td>Has Packet Data</td>
<td>--</td>
<td>Specifies if this log has associated packet data.</td>
</tr>
<tr>
<td>In Eth</td>
<td>--</td>
<td>The name of the Ethernet interface that receives packets transmitted from an external device.</td>
</tr>
<tr>
<td>Misc</td>
<td>--</td>
<td>A miscellaneous string associated with the current log.</td>
</tr>
<tr>
<td>NAT Dst Port</td>
<td>--</td>
<td>A destination port associated with the packet that has generated the log that has also undergone a network address translation.</td>
</tr>
<tr>
<td>NAT Src Port</td>
<td>--</td>
<td>A source port associated with the packet that has generated the log that has also undergone a network address translation.</td>
</tr>
<tr>
<td>NAT Dst Addr</td>
<td>--</td>
<td>A destination address associated with the packet that generated the log that has also undergone a network address translation.</td>
</tr>
<tr>
<td>NAT Src Addr</td>
<td>--</td>
<td>The source address associated with the packet that generated the log that has also undergone a network address translation.</td>
</tr>
<tr>
<td>Out Eth</td>
<td>--</td>
<td>The name of the Ethernet interface that transmits packets to an external device.</td>
</tr>
<tr>
<td>Packets In</td>
<td>--</td>
<td>Specifies the number of received packets for a given session on the current port.</td>
</tr>
<tr>
<td>Packets Out</td>
<td>--</td>
<td>Specifies the number of transmitted packets for a given session on the current port.</td>
</tr>
<tr>
<td>Packets Total</td>
<td>--</td>
<td>Specifies the aggregate number of both received and transmitted packets for a given session on the current port.</td>
</tr>
<tr>
<td>Policy</td>
<td>--</td>
<td>The name of the policy that generated the log.</td>
</tr>
<tr>
<td>Rule #</td>
<td>--</td>
<td>The rule in the rulebase in the policy in the specific version of a domain that generated this log.</td>
</tr>
<tr>
<td>Rule Domain</td>
<td>--</td>
<td>The domain that contained the rule that generated this log.</td>
</tr>
<tr>
<td>Rulebase</td>
<td>--</td>
<td>The rulebase inside the policy in a specific version of a domain that generated this log.</td>
</tr>
<tr>
<td>Time Generated</td>
<td>--</td>
<td>The time the current log was generated.</td>
</tr>
<tr>
<td>URI</td>
<td>--</td>
<td>Indicates the Universal Resource Indicator (URI) associated with the current log.</td>
</tr>
</tbody>
</table>
After importing a device configuration, log entries from that device begin to appear in the Log Viewer. However, until you update the device from NetScreen-Security Manager, the following log fields display 0 (or unknown):

- For 5.x devices: domain, domain version, rulebase, policy, rule number.
- For 4.0.x devices: domain, domain version, rulebase, policy, rule number, from zone, to zone, action.

After you update the imported device configuration using NetScreen-Security Manager, the appropriate values are displayed for log entries from the device.

**Log Viewer Detail Panes**

The Log Viewer contains additional panes that provide summary and detail information for log entry events. To see detailed information about a log entry, select the entry and view the detail panes at the bottom of the Log Viewer. The detail pane contains three tabs of information about the selected log record:

- **Summary tab (default tab)**—Details the event associated with the selected log entry. Within the summary tab, you can view the event description (right side) and the variable data (left side). Not all log entries contain variable data—only log entries generated by an attack provide variable data.
- **All Fields tab**—Provides a condensed view of data for the selected log entry (so you don’t need to scroll from horizontally).
- **Whois tab**—Enables you to perform a Whois lookup on an IP address to see what organization has registered a particular address.

**Log Viewer Status Bar**

The status bar of the Log Viewer summarizes the filters applied to log entries in the log entry list. In the status bar, the filter type description appears; to view filter details, place the cursor over the filter type.

For example, the status bar below displays the filter types Category and Severity:

<table>
<thead>
<tr>
<th>Column</th>
<th>Default</th>
<th>What it means</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Flag</td>
<td>–</td>
<td>The GUI assignable flag associated with the current log.</td>
</tr>
<tr>
<td>Vsys</td>
<td>–</td>
<td>The name of the virtual system that generated the current log.</td>
</tr>
<tr>
<td>Var Data</td>
<td>–</td>
<td>Indicates the kind of variable data if any associated with the current log.</td>
</tr>
<tr>
<td>Log ID</td>
<td>–</td>
<td>A value that represents the sequential record ID of the log for the specified day. In the format the n\text{th} log received.</td>
</tr>
</tbody>
</table>
Navigating the Log Viewer

Using the side scroll bar, you can navigate through hundreds of log entries quickly and precisely:

- Jump to top of log entry list (oldest logs)
- Page up within log entry list (older logs)
- Scroll up within log entry list (older logs)
- Scroll down within log entry list (more recent logs)
- Page down within log entry list (more recent logs)
- Jump to bottom of log entry list (most recent logs)

Log entries higher in the list are older than log entries at the bottom of the list. To navigate through log entries based on a specific time, use the Log Timeline (for details, see “Log Timeline” on page 741).

Searching Log Entries

The Log Viewer can receive thousands or even millions of log entries each day. To quickly locate a specific log entry or logs, use the following log searching tools:
Table 68: Search Tools for Log Viewer

<table>
<thead>
<tr>
<th>Tool</th>
<th>Description</th>
<th>Benefit</th>
</tr>
</thead>
</table>
| Log Timeline     | A 14-day timeline that enables you to zoom to log entries for a specific day and time. | - Specify an exact date and time, or use the timeline selection slider to move immediately to a specific day’s log entries.  
- Can also use the Tailing Logs feature to jump directly to incoming log entries.  
- Timeline covers any 14-day period, in increments of days, hours, or minutes. |
| Flags            | A symbol used to tag a specific log entry that you want to return to at a later point. The flagged entry stands out from other entries, making it easier to locate quickly. | - Gain greater control over identifying events.  
- Flags are colorful and iconic, making them more visible than text-based results of filters.  
- You can filter on a flag setting. |
| Find Utility     | A string search that searches for a log entry based on a character string in the reported event. | - Locate a specific event quickly with minimal detail; for example, search using the timestamp or IP address field.  
- Move quickly from one relevant event to another, avoiding scrolling. |
| Log ID Number    | A value search that searches for a log entry based on the log ID number.       | Locate a specific log entry immediately. Typically, you use a log ID search when you have previously viewed the log entry and need to find it again quickly. |

The following sections detail each search tool.

Log Timeline

The log timeline is a powerful tool that enables you quickly jump to a group of log entries generated during a specific time period.

The timeline consists of 4 components: the time slider, time entry, time blocks, and Tailing Logs. The following sections detail each component.

Using the Time Slider

The time slider marks the midpoint of the time interval selected for the timeline (for details on setting a time interval, see “Using Time Blocks” on page 742). You can move the time slider to the desired time using your mouse cursor: Click the slider, then drag it to the area on the timeline that represents the time around which you want to view log entries, as shown below:
Using Time Entry

You can also enter a date and time into the log timeline directly. Select the time display, then enter the desired time and click Go.

Using Time Blocks

To change the log timeline intervals, select a specific time block or use the Out and In buttons. From left to right, the time blocks are:

- 14 days
- 7 days
- 3 days
- 1 day
- 12 hours
- 6 hours
- 3 hours
- 1 hour
Using the Log Viewer

Chapter 12: Logging

Clicking the Out button selects the time block to the left of the currently selected time block; clicking the In button selects the time block to the right of the currently selected time block. Alternatively, you can use the mouse wheel on your mouse to adjust the time interval.

Using Tailing Logs
To view arriving log entries, select Tailing Logs. The log entry list automatically jumps to the bottom of the list, where new log entries display when they are received by the management system. As older log entries are moved up by arriving log entries, the view remains fixed at the bottom of the list.

Tailing Logs also works with filters, predefined view, and custom views.

EXAMPLE: TAILING INCOMING LOGS IN THE LOG VIEWER
To see configuration log entries as they arrive from a specific device:

1. Select the 7-Config view from the Log Viewer navigation tree. This view uses a predefined filter to display log entries with the category “configuration” only.

2. Set a custom filter to set log entries from a specific device (for details, see “Filtering Log Entries by Event and Time” on page 744). The view changes to display configuration log entries from that device.

3. Select Tailing Logs. The view jumps to the bottom of the log entry list, and remains there; as new configuration log entries for the device arrive, they appear at the bottom of the list.

Using Flags
Use a flag to mark a specific event with a severity or workflow marker. Applying a flag to a log entries helps the event stand out from other log entries. The following table displays a list of log filter symbols.

Table 69: Log Viewer Flags

<table>
<thead>
<tr>
<th>Filter Symbol</th>
<th>Severity Level</th>
<th>Filter Type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Low</td>
<td>Severity</td>
</tr>
<tr>
<td></td>
<td>Medium</td>
<td>Severity</td>
</tr>
<tr>
<td></td>
<td>High</td>
<td>Severity</td>
</tr>
</tbody>
</table>
Using the Log Viewer

Within the Log Viewer, you can set a filter on one or more flags. Additionally, within Report Manager, you can generate a report that displays the count of all log entries that contain a specific flag.

**Using the Find Utility**

Use the Find utility to search for the next iteration (down) of a value in the Log Viewer. To use Find on a column or cell, right-click the column header or cell and select Find, then configure the search criteria. Select Negate to search for all log entries that do not contain the specified value.

**Using Log ID Number**

When you know the Log ID number for the log entry, you can jump directly to the log entry. To locate a log entry by Log ID number, from the file menu, select Edit > Go To Log ID. In the Go To Log ID dialog box, enter the log ID number click OK. The Log Viewer jumps to the specified Log ID and highlights the log entry in the main display area.

**Filtering Log Entries by Event and Time**

An event- or time-based filter is a criteria search for matching log entries. When you apply a filter to log entries, the Log Viewer filters out log entries that do not match the filter criteria. You can set multiple filters on any Log Viewer column (except Log ID and Details) or cell value.

When filtering by cell, the filter affects only the content in that cell’s column. To set a cell filter, right-click a cell and select Filter to display the filter menu options:

- **Edit**—Use this option to set multiple filters for cell content at the same time. Select to display the Filter dialog box for that column, then select the columns you want to filter on.
  - To display only the selected content, click OK.
To display everything except the selected content, click the checkbox next to Negate, then click OK.

To clear filters for the selected content, click Clear.

Only This Value—Displays only the content in the selected cell.

Not This Value—Displays everything except the content in the selected cell.

Clear Filter—Removes a current filter on the selected cell content. If no filter exists, this option is unavailable.

Clear All Filters—Removes all filters on the current view.

When filtering by column, the filter affects all log entries. You can set an event-based filter using any log entry column that contains event data, and a time-based filter for the Time Generated and Time Received columns. Additionally, for all filters (cell or column), you can enable the Negate option to match all log entries that do not contain the specified filter criteria.

NOTE: You cannot apply a filter to the Log ID or Details column.

The following sections detail some common event- and time-based filters used to manage log entries.

Setting a Category Filter

Apply a category filter to view log entries within a specific category or subcategory.

To create a category filter, right-click the Category column header and select Filter > Set Filter. Select the categories you want to use as the filter criteria, then click OK. NetScreen-Security Manager applies the filter to all log entries and displays only the log entries that match the specified category.

To create a subcategory filter, right-click the Subcategory column header and select Filter > Set Filter. Select the category first, then select the subcategories you want to use as the filter criteria, then click OK. NetScreen-Security Manager applies the filter to all log entries and displays only the log entries that match the specified subcategory.

Setting an Alert Filter

Apply an alert filter to view log entries that have an enabled or a disabled alert state.

To create an alert filter, right-click the Alert column header and select Filter > Set Filter, then configure the alert filter settings:

To display log entries that contain an enabled alert, select On and click Ok.

To display log entries that contain a disabled alert, select Off and click Ok.

NetScreen-Security Manager applies the filter to all log entries and displays only the log entries that match the specified alert state.
Setting a Flag Filter

Apply a flag filter to view log entries that have a specified flag type. To create a flag filter, right-click the Flag column header and select Filter > Set Filter. Select the flag types that you want to use as the filter criteria, then click OK. NetScreen-Security Manager applies the filter to all log entries and displays only the log entries that match the specified flag type.

NOTE: The Unflagged option in the flag filter can be helpful when trying to locate log entries that do not have assigned flags. When setting the flag criteria, select Unflagged as the flag type; NetScreen-Security Manager then displays all log entries without flags.

Setting an Address Filter

Apply an address filter to view log entries that record events for a specific source or destination address, or source or destination NAT address. To create an address filter, right-click the Src Addr, Dst Addr, NAT Src Addr, or NAT Dst Addr column header and select Filter > Set Filter. Select “Click here to add address” and enter a valid IP address and click Ok. For NAT addresses, enter the IP address that is translated and click Ok.

NetScreen-Security Manager applies the filter to all log entries and displays only the log entries that match the specified IP address.

Setting a Protocol Filter

Apply a protocol filter to view log entries for events that use a specific protocol type. To create a protocol filter, right-click the Protocol column header and select Filter > Set Filter. Select the protocol types that you want to use as the filter criteria, then click OK. NetScreen-Security Manager applies the filter to all log entries and displays only the log entries that match the specified protocol types.

Setting a Domain Filter

The Log Viewer displays log entries for a single domain at time. By default, when logged in as the super admin, the Log Viewer displays log entries for managed devices in the global domain. To change the domain, apply a domain filter to view log entries for managed devices in a specific domain.

To create a domain filter, right-click the Domain column and select Filter > Set Filter. Select the domain for which you want to view log entries, then click OK. NetScreen-Security Manager applies the filter to all log entries and displays only the log entries that are generated from managed devices in the specified domain.

Setting a Time-Based Filter

Apply a time-based filter to view log entries generated or received within a specific time period. To create a time-based filter, right-click the Time Generated or Time Received column and select Filter > Set Filter:

- To filter on a specific start time, select From and configure the start date and time. When applied, this filter displays log entries for events that were generated or received after or at the specified start time.
To filter on a specific end time, select To and configure the end date and time. When applied, this filter displays log entries for events that were generated or received before or at the specified end time.

To filter on a time period, select From and To, then enter the start and end date and time. When applied, this filter displays log entries for events that were generated or received within the specified time period.

EXAMPLE: USING FILTERS IN THE LOG VIEWER
In this example, you want to view all critical and major severity log entries that have a Follow-Up flag assigned to them. Additionally, you want to limit the search to log entries generated by the Engineering NSRP cluster on your network.

1. In the Log Viewer, right click the severity column header and select Filter > Set Filter. Enable Major and Critical, then click to save and apply the filter to your log entries.

2. Right click the User Flag column header and select Filter > Set Filter. Enable Follow-Up, then click OK to save and apply the filter to your log entries.

3. Right click the Device column header and select Filter > Set Filter. Select Engineering Cluster, then click OK to save and apply the filter to your log entries.

Filtering Log Entries by Range

A range filter is a criteria search for matching log entries within a value range. You can set a range filter for the following columns:

- Bytes In/Bytes Out
- Bytes Total
- Packets In/Packets Out
- Packets Total
- Src Port/Dst Port
- NAT Src Port/NAT Dst Port
- Elapsed Seconds

The following sections detail some common range filters used to manage log entries.

Setting a Bytes In/ Out Range Filter

To view log entries based on the number of bytes received or transmitted during the event, set a range filter on the Bytes In or Bytes Out column:
1. Right-click the Bytes In or Bytes Out column header and select Filter > Set Filter. The Bytes In/Bytes Out filter dialog box appears.

NOTE: By default, the Log Viewer does not display the Bytes In or Bytes Out column. To set a byte filter, you must first configure the Log Viewer to display these columns. For details on configuring column settings, see “Customizing Columns” on page 748.

2. Set the range for bytes received (Bytes In) or transmitted (Bytes Out):
   a. To filter on a minimum number of bytes only, select From and enter a value. When applied, this filter displays log entries for events that received or transmitted more than or equal to the specified minimum number of bytes.
   b. To filter on a maximum number of bytes only, select To and enter a value. When applied, this filter displays log entries for events that received or transmitted fewer than or equal to the specified maximum number of bytes.
   c. To filter on a range of bytes, select From and To, then enter the minimum and maximum values for the range. When applied, this filter displays log entries for events that received or transmitted a number of bytes within the specified range.

3. Click OK to apply the filter.

Setting a Port Number Range Filter
To view log entries based on a range of port numbers used in the event, set a range filter on the Dst or Src Port column:

1. Right-click the Src Port or Dst Port column header and select Filter > Set Filter. The Dst/Src Port filter appears.

2. Set the range for the port numbers:
   a. To filter on a minimum port number only, select From and enter a value. When applied, this filter displays log entries for events that used a port greater than or equal to the specified minimum port number.
   b. To filter on a maximum port number only, select To and enter a value. When applied, this filter displays log entries for events that used a port less than or equal to the specified maximum port number.
   c. To filter on a range of port numbers, select From and To, then enter the minimum and maximum values for the range. When applied, this filter displays log entries for events that used ports within the specified range.

3. Click OK to apply the filter.

Customizing Columns
You can configure the Log Viewer to display specific columns.
Using Column Settings

The Log Viewer includes 40 columns of log entry information; however, each predefined view includes only a small subset (16) of available columns. To view information in the other available columns, or to change the column display order, you can adjust the column settings for the view.

The more columns you configure to appear in the Log Viewer, the more information you can see at one time—and the more you must scroll from side to side to view all columns; setting fewer columns means less viewable information, but also less scrolling. Typically, you use fewer columns when you already have enough detail about the event and/or you are only interested in specific event data.

Use column selection in combination with filters to create a customized view of your log entries.

Hide/ Unhide/ Move Columns

You hide, unhide, or move columns to display specific information using one of the following methods:

- When managing columns using the Column Settings dialog box:
  - To display hidden columns, select the columns and click Show.
  - To hide columns, select the columns and click Hide.
  - To reorder the column display sequence, select a column and click Move Up and Move Down.

- When managing columns in the main display area:
  - To hide a column, right-click the column header and select Hide Column. To unhide a hidden column, you must use the Column Settings dialog box.
  - To reorder the column display sequence, select a column and drag it to the new location.
  - To change column width, select the left or right edge of the column header and drag the edge to the desired width.

Example: Customizing Log Viewer Columns

In this example, you want to view the following information in the Log Viewer:

- The attacks that attempt to enter your network.
- The source IP and port of the attacking computers.
- The destination IP and port on the target computers.
- The date and time of the attacks.
- The devices that detected the attack.
- The policies that matched the attack.
First, you configure the Log Viewer to display only the columns that contain the information you are interested in viewing, then you set can filters on those columns to narrow your search.

To configure the column settings:

1. In the navigation tree, select the Log Viewer module.
2. From the file menu, select View > Choose Columns. NetScreen-Security Manager displays the Column Settings dialog box, listing all 40 columns.
3. Select the following columns:
   - Time Received
   - Src Addr
   - Dst Addr
   - Dst Port
   - Category
   - Subcategory
   - Device
   - Policy
   - Src Port

   Ensure all other columns are not selected, then click OK to apply your changes to the Log Viewer.
4. In the main display area, select the Src Port column header, then drag and drop the column to the right of the Src Addr column.

To configure the column filters:

1. In the main display area, right-click the Category column header and select Filter > Set Filter. The Category filter dialog box appears.
2. Select the following categories: Predefined, Custom, and Screen. Click OK to apply your changes. The Log Viewer applies the filter to the log entries.

**Using Log Views**

The Log Viewer includes several predefined views for critical severity attacks, configuration log entries, scans, and other important activities. Using filters, you can create your own unique, customized log entry view, then save the custom view (with all its filters) for future use.
Creating Custom Views

A custom view enables you to organize log entries in a format that is most helpful to you. Because the custom view is based on filters, incoming log entries that match the filter criteria are automatically displayed in the view (you do not need to re-apply the view to new logs).

You might want to create views to help manage the following situations:

- **Workflow**—To help a team of security administrators work together to investigate and resolve incidents, create a view that filters on the flag column of the Log Viewer to indicate the status of each log entry and assignment.

- **Attackers**—To track the activities of a known attacker, create a view that filters on a specific source IP. The source IP address of an attack displays in the source address column, and the destination IP address of an attack displays in the destination address column.

- **Alarms**—To quickly access log entries generated by a policy rule that contains an alarm, create a view that filters on the alarm column. This method is useful when you are fine-tuning policies to distinguish between genuine attacks and false positives.

- **Devices**—To manage devices in multiple locations that use different investigation processes, create a separate view for each device at a specific location.

You can create and save custom views using one of the following methods:

- **Create New View**—First In the navigation tree, select the Log Viewer module. From the file menu, select File > New View. In the new view dialog box, enter a name for the custom view and click OK; the new view appears in the navigation tree, at the bottom of the predefined view list. In the main display area, set the desired filters for the log entries.

- **Set Filters**—First In the Log Viewer main display area, set the desired filters for the view. From the file menu, select File > Save As. In the new view dialog box, enter a name for the custom view and click OK; the new view appear in the navigation tree, at the bottom of the predefined view list.

**Exporting Views**

To save a predefined or custom view to a specific format, you can export the view to an Adobe PDF file or a standard PostScript file. For step-by-step instructions on exporting a view, see the NetScreen-Security Manager Online Help topic “Exporting from the Log Viewer”.

---

**NOTE:** The Log Viewer can only export a maximum of 77 logs to the PDF/PostScript file.
Using Log Viewer Integration

The Log Viewer module is integrated with Security Policies and Device Manager modules. This integration enables you to jump from a log entry in the Log Viewer directly to the responsible Security Policy (Jump to Rule) or managed device (Jump to Device Configuration).

Jump to Policy
To quickly edit a Security Policy rule from the Log Viewer, right-click a log entry and select Jump to Policy. NetScreen-Security Manager opens a new UI window and displays the policy with the rule that generated the log entry.

- If the responsible rule exists within a rule group, the group is automatically expanded to reveal the rule.
- If the responsible rule exists within a VPN created by VPN Manager, the autogenerated rules appear.

Depending on the domain version of the Security Policy, the rule might display as read/write or read-only.

Domain version refers to a specific modeled configuration; each time you install a modeled configuration (this includes Security Policies) on a managed device using NetScreen-Security Manager, the management system creates a new domain version using the install date and time. NetScreen-Security Manager uses domain versions to detect differences between the running configuration (installed on the physical device) and modeled configuration. Domain versioning also enables you to view previous domain versions. For details on domain versions, see “Domain Versioning” on page 65.

Other options for archiving and restoring logs and configuration data are also available. For more information, refer to the NetScreen-Security Manager Installer Guide.

When using the Jump to Policy option in the Log Viewer, NetScreen-Security Manager compares the domain version of the managed device to the current domain version. If the responsible rule exists in a Security Policy that has the same domain version as the Security Policy installed on the managed device, you can edit the rule.

However, if the responsible rule exists in a Security Policy that has a different domain version from the Security Policy installed on the managed device, you cannot edit the rule. This typically occurs when you install a Security Policy on a managed device, then edit that policy in the NetScreen-Security Manager UI but do not update the device with the new policy changes. Because the responsible rule exists in a policy that belongs to a previous domain version, you cannot make changes to it.

Jump to Device Configuration
To quickly configure a parameter on an individual device from the Log Viewer, double-click a device in the Device column. NetScreen-Security Manager displays the device configuration for the device, enabling you to make changes to the device.
Identifying Irrelevant Attacks

Your log entries are a valuable tool in helping you identify irrelevant attacks. Irrelevant attacks are events that do not affect your network or that you do not consider important. Typically, you want to identify irrelevant attacks to:

- Reduce the number of log entries and increase system performance.
- Isolate log entries for harmless attacks.
- Focus on log entries for attacks to which you are actually vulnerable.

Select a log entry generated by a protocol anomaly or signature attack object, then view the Summary panel to see the attack description. An example is shown below:

Figure 201: Viewing Summary Panel

Look carefully at the information about affected systems, and compare it with what you know about your network. Use the following information to help you determine if the attack is relevant:

Table 70: Irrelevant Vs. Relevant Attacks

<table>
<thead>
<tr>
<th>Irrelevant Attacks</th>
<th>Relevant Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack target hardware you do not use.</td>
<td>Attack attempts to exploit vulnerabilities in the hardware you use in your network.</td>
</tr>
<tr>
<td>Example: Attacks that exploit Cisco routers do not affect Lucent routers.</td>
<td></td>
</tr>
<tr>
<td>Attack target software you do not use.</td>
<td>Attack attempts to exploit vulnerabilities in the software running on your network.</td>
</tr>
<tr>
<td>Example: Attacks that exploit Microsoft IIS Web servers do not affect Apache Web servers.</td>
<td></td>
</tr>
<tr>
<td>Attack target software versions you do not use.</td>
<td>Attack attempts to exploit vulnerabilities in the software versions running on your network.</td>
</tr>
</tbody>
</table>

If the attack is irrelevant, you can remove the matching Attack Object group from the rule that triggered the log entry, or monitor the Attack Object group using custom severity setting.
Using the Log Investigator

The Log Investigator module enables you to investigate patterns and trends on your network using data gathered from your log entries. Log entries are generated by a security device when traffic matches a Security Policy rule, or when an event occurs that matches a predefined set of conditions. The Log Investigator uses the event data recorded in the log entry to identify the destination IP addresses and ports that are attacked most frequently, the services that are used to attack most frequently, and the source IP addresses that most frequently generate attacks.

When using NetScreen-Security Manager to manage large networks with multiple managed devices, you can potentially receive several hundred log entries in a single day (depending on how you have configured your devices for logging). The Log Investigator is a helpful tool for manipulating and correlating a large volume of log entry data so you can identify and analyze important activity that might threaten your network. By analyzing your data and then using that knowledge to proactively fine-tune your Security Policies, you can decrease risk while increasing security.

This section provides details on the following Log Investigator functionality:

- **About the Log Investigator UI**—The Log Investigator main display area includes a filter summary, a log entry matrix, and two detail panes that display detail information in table and chart format.

- **Configuring Log Investigator Options**—Configure the criteria the Log Investigator uses to create the matrix, including the time period, Left and Top Axes settings, the data point count (the number of data points the Log Investigator must collect before displaying data), and the maximum number of log entries you want the Log Investigator to use when collecting data.

- **Setting Log Investigator Filters**—As in the Log Viewer, you can set filters on log entry data so the Log Investigator displays only the information you want to see. Apply multiple filters to data for all log entry columns found in the Log Viewer.

- **Investigating Log Entry Data**—After you have configured the Log Investigator filters, time period, and data options, you are ready to begin investigating your log entry information. Within any cell the Log Investigator table, you can right-click and select an option to view specific details, including Destination Ports, Subcategories, and Time Period.

**About the Log Investigator UI**

The main display of the Log Investigator is shown below:
The Log Investigator contains the following UI components:

- **Filter Summary**—Displays the column/category filters currently applied to the Log Entry Matrix.

- **Selected Log Entries**—Displays the number of log entries currently selected in the Log Entry Matrix.

- **Left Axis**—The controlling axis for log entry data (the independent axis). The Log Investigator collects log entry data for the Left Axis setting, which determines data set that is used for Top Axis setting.

- **Top Axis**—The controlled axis for log entry data (the dependent axis). The Log Investigator collects log entry data for the Left Axis setting; for the Top Axis setting, the Log investigator collects data that matches both the Left Axis and Top Axis setting.
- **Zoom Table**—Displays a table of log entry details. You can view Source, Destination, Destination Port, Attack Subcategories, or Time Period details for any cell, row, or column.

- **Zoom Chart**—Displays a chart of log entry details. You can view Source, Destination, Destination Port, Attack Subcategories, or Time Period details for any cell, row, or column.

### Configuring Log Investigator Options

The first step in using the Log Investigator is to configure the basic criteria used to create the Log Investigator matrix. Initially, the default options are used; to edit these options, from the file menu, select View > Set Log Investigator Options. Using the Log Investigator Options dialog box, configure the desired settings (detailed below) and click OK to apply your changes.

![NOTE:](image)

You can configure up to 20 Log Investigator sessions. To change this default number of sessions, edit the following parameter in the devSvr.cfg file (located in the management system directory /usr/netscreen/DevSvr/var/):

```bash
devSvr.irMaxIndexCount
```

The following sections detail each Log Investigator option.

### Configuring a Time Period

The time period setting narrows the log entries included in your investigation based on a specified time interval or start time. Each log entry contains a timestamp that indicates the date and time the managed device generated the log entry (Time Generated). The Log Investigator compares the timestamp of a log entry to the specified time period setting, and eliminates those log entries that do not meet the time criteria.

First, you must specify a time duration. To specify a time interval for which you want to see log entries, set the number of weeks, days, hours, minutes, or seconds. Setting a longer interval time can help identify broad trends in your network activity. Typically, you want to use a longer interface time to initially locate problems. After you have identified the issues you want to investigate, set a shorter time interval to eliminate irrelevant log entry data.

After you have determined the time interval, you must set the end or start time for the duration:

- To set the end time of the duration, select Most Recent (this is the default setting). The Log Investigator uses the current date and time as the end point for the time duration. For example, for a time interval of 5 hours, the Log Investigator collects data from log entries that have timestamps within the previous 5 hours.

- To set the start time of the duration, select Start Time and configure the start date and time. The Log Investigator uses the specified date and time as the start point for the time duration. For example, for a time interval of 5 hours and a start date of 5/12/04 8:00:00AM, the Log Investigator collects data from log entries that have timestamps from the start date to the start date + 5 hours.
Typically, use Most Recent to investigate recurring activity or to monitor expected network changes. Use a start time when investigating past known events, such as a virus attack.

When using a large time interval, the number of matching log entries might exceed the capacity of the Log Investigator (100 log entries), causing a warning message to appear next to the Selected Logs indicator. If you do not make changes to the time interval filter, the Log Investigator automatically clears the session, requiring you to create a new time filter.

**EXAMPLE: SETTING A TIME INTERVAL IN THE LOG INVESTIGATOR**

On Friday afternoon, you want to investigate attacks received by your network in the last seven hours. Configure the time period as show below:

**Figure 203: Configure Time Period Filter**

```
<table>
<thead>
<tr>
<th>Time Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duration</td>
</tr>
<tr>
<td>7</td>
</tr>
<tr>
<td>hours</td>
</tr>
<tr>
<td>Most Recent</td>
</tr>
<tr>
<td>Starting at</td>
</tr>
<tr>
<td>5/21/04</td>
</tr>
<tr>
<td>12:00:00 AM</td>
</tr>
</tbody>
</table>
```

On Monday morning, you want to investigate attacks received by your network during the last work week. If Monday’s data is 5/17/04, you configure the time period as show below:

**Figure 204: Changing Time Period Filter**

```
<table>
<thead>
<tr>
<th>Time Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duration</td>
</tr>
<tr>
<td>5</td>
</tr>
<tr>
<td>days</td>
</tr>
<tr>
<td>Most Recent</td>
</tr>
<tr>
<td>Starting at</td>
</tr>
<tr>
<td>5/10/04</td>
</tr>
<tr>
<td>12:00:00 AM</td>
</tr>
</tbody>
</table>
```

**Configuring Axes**

The Left Axis is the independent axis because it is the first data collected. The Top Axis is dependent axis because it uses the Left Axis data as the data set.

The dependency occurs because the Log Investigator collects data that matches the Left Axis setting first; this data represents the data set for the entire log entry matrix. By default, the Left Axis is set to the data type Top Sources. After the Left Axis data set has been determined, the Log Investigator searches that data set for data that matches the Top Axis setting. By default, the Top Axis is set to the data type Top destinations.

Because the Left Axis setting controls the initial data set, it is the most important axis setting. Typically, you should set the Left Axis to the data type you most want to investigate.
Setting the Data Type
You can change the data type for each axis. The data type defines the type of information that the Log Investigator attempts to locate in your log entries. For either axis, you can set the following data types:

- **Top Sources**—The IP address that generated the event.
- **Top Destinations**—The IP address that received the event.
- **Top Subcategories**—The attack subcategory detected in the event.
- **Top Destination Ports**—The port numbers on the Destination device that received the event. The port number can help you identify the service used in the event.

By default, the Left Axis uses the data type Top Sources and the Top Axis uses the data type Top Destinations. To change these settings, simply select the desired data type in the data point source menu.

Setting Data Points
A data point is a single data type field that matches the axis setting. By default, each axis collects 10 data points for each evaluation. These default settings create a Log Entry Matrix of 100 cells (the top 10 source IP addresses are correlated against the top 10 destination IP addresses, creating a 100-cell matrix). For example, a data point count of 6 for each axis would create a 36-cell matrix).

You can set the data point higher (maximum 40) or lower (minimum 5), depending on your investigation requirements. To change these settings, simply select the desired data type in the data point count field. The higher the data count, the larger the log entry matrix—and the more processing power required by the Log Investigator UI. Using large data counts can slow performance.

EXAMPLE: USING LEFT AND TOP AXES IN THE LOG INVESTIGATOR
In this example, you configure swap the setting for the Left and Top Axes of the Log Investigator to see how each axis controls data.

Set the filter to Attacks, then configure the Left and Top Axes:

- To identify which of the most popular source addresses are generating attacks against the most popular destinations:
  - Select as the Left Axis (the independent axis) as Top Sources.
  - Select the Top Axis (the dependant axis) as Top Destinations.

The Left Axis displays all attacks for the Top Source IP addresses, while the Top Axis displays the number of attacks for each of the Top Destinations attacked by the Top Sources.

- To identify which of the most popular destination addresses are receiving attacks from the most popular sources:
  - Select as the Left Axis (the independent axis) as Top Destinations.
Select the Top Axis (the dependant axis) as Top Sources. The Left Axis displays all attacks against the Top Destination IP addresses, while the Top Axis displays the number of attacks for each Top Source IP address that attacked a Top Destination.

Setting a Log Entry Limit
You can limit the number of log entries used in Log Investigator calculations. The NetScreen-Security Manager Device Server stores log entries from managed devices and the management system; when the GUI Server accesses a log entry to display its information in the UI, that log entry is placed in a log buffer. As the Log Investigator searches your log database for log entries that match the filter, time period, and data type criteria, it places all matching log entries in the log buffer.

To control the size of this buffer (the number of matching log entries), you can configure the Max Log Count for your investigations. The limit defines the number of matching log entries the Log Investigator accepts for its calculations.

You can set the following log entry limits:
- 100,000 log entries
- 200,000 log entries
- 400,000 log entries
- 600,000 log entries
- 800,000 log entries
- 1,000,000 log entries

Be aware that setting a large buffer limit can cause the Log Investigator performance to degrade. The maximum buffer size of one million log entries uses all memory on the GUI Server and is not recommended.

**Setting Log Investigator Filters**

Log Investigator filters operate very similar to Log Viewer filters: You set criteria for log entries and the Log Investigator filters out log entries that do not match the filter criteria. Using the Filter Summary dialog box, you can select and apply multiple filters to the Log Investigator matrix.

To set filters, from the file menu, select View > Set Filter. The following table details filter types:
Table 71: Log Investigator Filters

<table>
<thead>
<tr>
<th>Filter Type</th>
<th>Sample Filters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Filters</td>
<td>Time Received</td>
<td>Identifies packets by the time when a packet is sent from a device and when a packet is received on a device.</td>
</tr>
<tr>
<td></td>
<td>Time Generated</td>
<td></td>
</tr>
<tr>
<td>Address Filter</td>
<td>Source Address</td>
<td>Identifies packets based on information about an address of a device from which the packet was sent or an address of a device to which the packet was sent.</td>
</tr>
<tr>
<td></td>
<td>Destination Address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device Address</td>
<td></td>
</tr>
<tr>
<td>Direction Filters</td>
<td>Inbound If</td>
<td>Identifies packets based on the direction they are heading to or from a specified device.</td>
</tr>
<tr>
<td></td>
<td>Outbound If</td>
<td></td>
</tr>
<tr>
<td>Device Filters</td>
<td>Device VIN</td>
<td>Identifies device ID number and virtual device value.</td>
</tr>
<tr>
<td></td>
<td>Virt Dev</td>
<td></td>
</tr>
<tr>
<td>Transmission Type Filters</td>
<td>Packets</td>
<td>Identifies transmissions based on whether they are seen as packets, bytes, or attacks.</td>
</tr>
<tr>
<td></td>
<td>Bytes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Attack</td>
<td></td>
</tr>
<tr>
<td>Port Filters</td>
<td>Src Port</td>
<td>Identifies packets based on the port on a device from where they were transmitted or on the port on a device to where they were transmitted.</td>
</tr>
<tr>
<td></td>
<td>Dst Port</td>
<td></td>
</tr>
<tr>
<td>Policy Filters</td>
<td>Policy ID</td>
<td>Identifies packets based on whether they meet the conditions of a policy or a rule.</td>
</tr>
<tr>
<td></td>
<td>Policy Version</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Rule Number</td>
<td></td>
</tr>
<tr>
<td>Alarm Filters</td>
<td>Flag</td>
<td>Identifies the severity level of a generated alarm.</td>
</tr>
<tr>
<td></td>
<td>Alarm</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td></td>
</tr>
<tr>
<td>Miscellaneous Filters</td>
<td>Protocol</td>
<td>Various</td>
</tr>
<tr>
<td></td>
<td>Category</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Email</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SNMP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Syslog</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td></td>
</tr>
</tbody>
</table>

**NOTE:** For a complete list of log entry columns available for filtering, see “Log Viewer Columns” on page 736.

After you have set a filter, the Filter Summary displays a list of all filters applied to the log entry data and the Log Investigator matrix displays values for matching log entries.

**EXAMPLE:** SETTING FILTERS IN THE LOG INVESTIGATOR

In this example, the Left Axis is set to Top Sources and the Top Axis is set to Top Destination (these are the default settings). To set a filter that displays all attack category log entries generated by the Top Sources and received by the Top Destinations:
1. From the file menu, select View > Set Filter to display the Filter Summary dialog box.

2. In the filter list on the left, select Category, then select the following categories in the right: Predefined, Custom, and Screen.

3. Click OK to save and apply your changes.

To view the number of attacks between a specific source-destination pair, locate the Source Address 63.172.115.190 and Destination Address 63.172.115.6, then find the cell where the two addresses intersect. The Log Investigator displays 140 log entries for this Source-Destination pair, as shown below:

Figure 205: View Log Investigator Results

<table>
<thead>
<tr>
<th>Source Address</th>
<th>Destination Address</th>
<th>63.172.115.190</th>
<th>63.172.115.6</th>
</tr>
</thead>
<tbody>
<tr>
<td>63.172.115.189</td>
<td>63.172.115.100</td>
<td>140</td>
<td></td>
</tr>
<tr>
<td>66.119.199.42</td>
<td>A.Toulouse-105.1-3-252.w80-11.abo.wanadoo.fr</td>
<td>26</td>
<td></td>
</tr>
<tr>
<td>blix.interl.net</td>
<td>164.164.94.253</td>
<td>13</td>
<td>14</td>
</tr>
<tr>
<td>mail.wirthware.com</td>
<td><a href="http://www.slicenet.org">www.slicenet.org</a></td>
<td>52</td>
<td></td>
</tr>
<tr>
<td>164.164.94.253</td>
<td>modem-221.babbelas.dialup.pol.co.uk</td>
<td>13</td>
<td></td>
</tr>
<tr>
<td><a href="http://www.rnc.org">www.rnc.org</a></td>
<td>cs66681127.austin.rr.com</td>
<td>26</td>
<td></td>
</tr>
</tbody>
</table>

This high value (140) reflects the number of attack log entries that have occurred between these two IP addresses.

Investigating Log Entry Data

After you have configured the Log Investigator options and set filters as desired, you are ready to begin investigating your log entry data.

Using Rows and Columns

Each row or column in the Log Entry matrix represents events for a single data type. When selecting a row/column, you are evaluating how the data type (source, destination, subcategory, or destination port) for that axis relates to the other axis during a specific time period. Typically, reviewing a row/column in the matrix helps you analyze all events for a single data type.
For example, to investigate a sudden drop in performance on a specific destination, set the Left Axis to Top Sources and the Top Axis to Top Destinations, then select the column for the destination IP address. For each cell that displays a high number of events received by that destination, locate the corresponding source IP address. You might determine that destination 1 is receiving a large number of events from source A, B, and C. This activity could be a harmless event, such as multiple users attempting to contact a single application server at the same time. You could eliminate the bottleneck by adding another application server to the network or restricting access to the existing server.

**Using Cells**

Each cell in the Log Entry matrix represents events that occur at the intersection of two data types. When selecting a cell, you are evaluating the events that occurred between those two specific data types (source, destination, subcategory, or destination port) during a specific time period. Typically, reviewing a cell in the matrix helps you analyze all events that occur between a data type pair.

For example, to investigate a sudden drop in network performance, set the Left Axis to Top Sources and the Top Axis to Top Destinations, then review the log entry matrix to locate a large number for a location pair. You might identify that source A is sending an unusually large number of transmissions to destination 1. This activity could be a harmless event, such as an employee archiving multiple large files before leaving work; however, this activity might be the result of a denial-of-service attack triggered by an internal trojan. You probably need to get more details, such as destination ports used and attack subcategories for the events before you can resolve the issue.

The following table details the benefits of each type of Log Investigator analysis.

**Table 72: Log Investigator Analysis**

<table>
<thead>
<tr>
<th>Data Type A (Left Axis)</th>
<th>Data Type B (Top Axis)</th>
<th>Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiple Rows</td>
<td>Multiple Columns</td>
<td>View all network activity for specific data types. No cells or columns are selected (default view). Useful for analyzing events for multiple data types, such as multiple destinations and multiple sources. To focus on a specific data type pair, select the intersection cell.</td>
</tr>
<tr>
<td>Multiple Row</td>
<td>One Column</td>
<td>View network activity for a single data type. A single column is selected. Useful for analyzing network performance issues, such as multiple sources generating traffic to a single destination.</td>
</tr>
<tr>
<td>One Row</td>
<td>Multiple Column</td>
<td>View network activity for a single data type. A single row is selected. Useful for analyzing attack traffic, such as one source generating traffic to multiple destinations.</td>
</tr>
<tr>
<td>One Row</td>
<td>One Column</td>
<td>View specific activity between two specific data types. A single cell is selected. Useful for analyzing event traffic between two network components.</td>
</tr>
</tbody>
</table>
Zoom Details

You can zoom in on specific details about activity between two data types. You can select a third data type for comparison, or display details about the event over time. To get details, right-click a cell, row, or column and select Zoom In to see the list of available data types. Because the Zoom In menu is dynamic, it contains all data types not currently used for the Left or Top Axis of the Log Investigator matrix. Alternatively, you can select time as the third data type.

Details appear in the Zoom area, which contains two panes:

- The Zoom table (left pane)
- The Zoom chart (right pane)

The table and chart use the same information to generate values.

EXAMPLE: VIEWING DESTINATION PORTS IN THE LOG INVESTIGATOR

In this example, the Left Axis is set to Top Sources and the Top Axis is set to Top Destination (these are the default settings); the filter is set to attacks (for details on setting the filter, see “Setting Filters in the Log Investigator” on page 760).

To view the service ports on the destination device used by the attacks, right-click a cell that contains a non-zero value and select Zoom In > Dst Port. In the Zoom area:

- The left pane displays a table of service ports listed in descending order (the port accessed by the most attacks is listed first). The left column lists the Destination Port Number and the right column lists the number of attacks received by that port number. Because services are mapped to specific port numbers, you can use the port number to identify the service used in the attack.

- The right pane displays a chart using the same information.

EXAMPLE: VIEWING SUBCATEGORY DETAILS IN THE LOG INVESTIGATOR

In this example, the Left Axis is set to Top Sources and the Top Axis is set to Top Destination (these are the default settings); the filter is set to attacks (for details on setting the filter, see “Setting Filters in the Log Investigator” on page 760).

To view the individual attacks (the attack subcategories) against the destination device, right-click a cell that contains a non-zero value and select Zoom In > Subcategory. In the Zoom area, the left pane displays a table of attack subcategories listed in descending order (the attack found in the most number of log entries is listed first); the right pane displays a chart using the same information.

EXAMPLE: VIEWING TIME PERIOD IN THE LOG INVESTIGATOR

In this example, the Left Axis is set to Top Sources and the Top Axis is set to Top Destination (these are the default settings); the filter is set to attacks (for details on setting the filter, see the example “Setting Filters in the Log Investigator” on page 760).
To view the time period over which the attacks occurred, right-click a cell that has a non-zero value and select Zoom In > Time. In the Zoom area, the left pane displays a table of attacks listed in order (the oldest attack is listed first); the right pane displays a chart using the same information.

Jumping to the Log Viewer

The Log Investigator uses log entry data for calculations, and does not display the actual log entries. However, you can use the Log Viewer to see the log entries used in Log Investigator calculations.

To see corresponding log entries, right-click a cell, row, or column from the Log Investigator matrix or the Zoom table and select View in Log Viewer. NetScreen-Security Manager creates a new UI window that displays the log entries in the Log Viewer.

Excluding Data

You can manually configure the Log Investigator to exclude data for a cell, row, or column in the Log Investigator matrix. You might want to exclude:

- Irrelevant values (such as values from sources or destinations no longer in production)
- Abnormally high or low values (to establish a baseline)
- Specific data type (source, destination, destination port, subcategory)
- High values (when investigating events that generate lower values)

To exclude a specific attack from the Log Investigator calculations, right-click the attack cell and select Exclude. To help you keep track of excluded values, the Filter Summary area displays a list of values you have manually excluded.

Using the Audit Log Viewer

The Audit Log Viewer monitors administrative events that occur when a NetScreen-Security Manager administrator makes changes to a domain. Use the Audit Log Viewer to track changes to your managed device configurations. You can view audit log entries for all managed devices in the all domains you have access to, or simply view entries for the devices in a single domain.

The Audit Log Viewer appears as the last module in the NetScreen-Security Manager UI. Select the Audit Log Viewer to display the audit log entry table, device view, and target view, as shown below:
Audit Log Table

The audit log table contains the following columns of information:

Table 73:  Audit Log Information

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Generated</td>
<td>The time the object was changed. The Audit Log Viewer displays log entries in order of time generated by Greenwich Mean Time (GMT).</td>
</tr>
<tr>
<td>Admin Name/Domain</td>
<td>The name of the NetScreen-Security Manager administrator who changed the object and the name of the domain (Global or Subdomain) that contains the changed object.</td>
</tr>
<tr>
<td>Action</td>
<td>The type of change applied to the object. For a complete list of the actions that Audit Log Viewer tracks, see “Audit Log Entry Actions” on page 766.</td>
</tr>
<tr>
<td>Target Object Type/Name/Domain</td>
<td>For changes made to a device configuration or object, the Audit Log Viewer displays the object type, the object name, and the object domain.</td>
</tr>
<tr>
<td>Device Name/Type/Domain</td>
<td>For changes made to the device, the Audit Log Viewer displays the device name, the object type, and the device domain. For changes made to the management system, such as administrator login/logout, the Audit Log Viewer does not display target or device data.</td>
</tr>
<tr>
<td>Log ID</td>
<td>The assigned log ID number.</td>
</tr>
</tbody>
</table>
For changes to devices or device configuration, you can use the Target View and/or Device View to get more details about those changes.

Target View and Device View

The Audit Log Viewer also contains two detail views:

- **Target View**—For a change made to the device configuration, such as changing an IP address or renaming the device, select the audit log entry for that change in the audit log table, then view the Target View to see details about that change.

- **Device View**—For a change made to the device itself, such as adding the device, autodetecting a device, or rebooting a device, select the audit log entry for that change in the audit log table, then view the Device View to see details about that change.

To see additional details for a target or device audit log entry, double-click the entry in the Target or Device View. For Target, NetScreen-Security Manager displays the configuration screen that the change was made in and marks the changed field with a solid green triangle. For Devices, NetScreen-Security Manager displays the Job Manager information window for the job task.

Setting a Start Time for Audit Log Entries

By default, the Audit Log Viewer displays audit log entries in order of time generated by Greenwich Mean Time (GMT). To configure the Audit Log Viewer to display log entries for events that occurred after a specific time, configure the Log By Time option.

From the menu bar, select View > Go To Log By Time to display the Log By Time dialog box. Select a date and time, then click OK to save and apply the time change to the Audit Log Viewer. The audit log table now displays only the audit log entries that were generated on or after the date and time you specified.

Audit Log Entry Actions

The Audit Log records the following administrative actions:

- Add device
- Autodetect device
- Get configuration summary
- Get delta configuration summary
- Update device
- Reboot device
- Import configuration
- Import configuration offline
- Get running configuration summary
- Delete certificate
- Refresh certificate list
- Flash synchronization
- Set root admin
- Failover status
- Failover revert
- Rule validation summary
- Upload fulfilled certificate
- Generate certificate
- Install software key
- DNS refresh
- NTP update
- Generate preshared key
- Modify BGP peer session
- DI attack update
- DI attack check
- Scan manager pattern update
- Get rule validation summary
- Get policy list
- Import vsys device
- Import cluster member
- Delete vsys device
- Get license key info
- Auto detect vsys
- Policy merge
- Update firmware
- Configuration verification
- Update configuration
Managing Log Volume

Security administrators have different requirements for how many log entries they need to keep. Some administrators must keep all log entries as directed by their corporate Security Policy, resulting in large numbers of log entries that the administrator might not have time to review, but need to store.

To manage log volume, you can:

- Archiving Logs
- Purging Logs

**NOTE:** Excessive logging creates additional traffic on your network. We recommend balancing your logging needs with the performance needs of your management system.

You can also export your log records to other formats for use in other applications. For details on how to forward logs, see “Forwarding Logs” on page 769.

**Archiving Logs**

You can archive and retrieve log entries to and from a storage device using standard Unix commands.

Logs reside on the Device Server in the following directory:

`/usr/netscreen/DevSvr/var`

We recommend using the following commands to archive your logs:

- The `tar` command
- The **scp** (Secure Copy) command
- The **ftp** (File Transfer Protocol) command

For full descriptions and options for each command, see the man pages.

---

**NOTE:** You **do not** need to stop the processes on the Device Server before archiving.

---

### Purging Logs

The Device Server maintains a minimum of 1000Mb (by default) of disk space available, primarily for the storage of log records. When the available disk space reaches this minimum, it sends an email alerting you of the situation.

**NOTE:** Use the Server Manager node in the NetScreen-Security Manager UI to configure email notification. Refer to “Configuring Servers” on page 711 for more information.

In the event that disk space on the Device Server reaches a minimum of 500Mb, the Device Server attempts to free the disk space by purging log records beginning with the oldest records on file. The Device Server stops purging log records when the 1000Mb minimum disk space is restored. If for any reason, the Device Server is not able to restore 500Mb of disk space, the Device Server will automatically shut down. If the Device Server fails to restart for this reason, an error message appears in the console window indicating that there is not enough disk space on the server machine, and that you must either backup your data or free up additional disk space in order to start the server again.

If you want to change the parameters for managing disk space on the Device Server, you can edit the Device Server configuration file. For more information on configuring the minimum disk space available on the Device Server, refer to the NetScreen-Security Manager Installer’s Guide.

---

### Forwarding Logs

You can forward your log records for use in other applications using one of the following methods:

- **Action Manager**—use the Action Manager, a node on the main UI, to configure the management system to forward logs generated within a specific domain or subdomain in NetScreen-Security Manager.

- **Log2Action utility**—a command line utility located on the NetScreen-Security Manager Device Server.

**NOTE:** You can also forward logs based on specific rules in a security policy. Refer to Configuring Firewall Rules on page 527 for more information.
Using the Action Manager to Forward Logs by Domain

Use the Action Manager node to configure the management system to perform actions (such as syslog, export, or alarm) on log data based on the criteria you specify. These actions occur for all the managed security devices in a specific domain or subdomain.

To enable the management system to export logs, you must configure the following:

- **Action Parameters**—These settings define the default log export settings for the management system, and determine how the system handles qualified log entries (log entries that match specified log criteria).
- **Device Log Action Criteria**—The criteria specifies the category and severity of the log entries you want to export. When a log entry meets the specified criteria, it is considered qualified, and NetScreen-Security Manager performs the specified actions defined in the criteria.

Configuring Action Parameters

From the Action Manager, select Action Parameters to define the default log export settings for the management system. To enable the management system to export qualified logs to Syslog, SNMP, CSV, XML or email, configure the export settings for each format as detailed in the following sections.

**Exporting to Syslog**

For exporting to syslog, configure the IP address and the server facility for the syslog server to which you want to send qualified logs. NetScreen-Security Manager uses this server when exporting qualified log entries to syslog.

This setting simply defines the syslog settings for the management system. To actually export logs to the syslog server, you must select “Syslog Enable” using the Actions tab in the Device Action Log Criteria node.

**Exporting to SNMP**

For exporting to SNMP, configure the following SNMP settings:

- **SNMP Manager**—Specify the IP address of the SNMP server to which the GUI Server sends SNMP traps.
- **SNMP Community**—Specify an SNMP community name that provides a desired combination of both read and write access from the SNMP server.

NetScreen-Security Manager uses this information when exporting qualified log entries to SNMP. This setting simply defines the SNMP settings for the management system. To actually export logs to the specified SNMP server and community, you must select “SNMP Enable” using the Actions tab in the Device Action Log Criteria node.

**NOTE:** The NSM MIB file resides in the /usr/netscreen/DevSvr/utils directory on the management system, and the file name is jnx-nsm-traps.mib.
Exporting to CSV
For exporting to CSV, configure the following CSV settings:

- File Path—The directory and filename that you want log entries exported to in .CSV format.
- Print Header—When selected, column headers are exported to .CSV format.

NetScreen-Security Manager uses this information when exporting qualified log entries to CSV. This setting simply defines the CSV settings for the management system. To export logs to CSV, you must select “CSV Enable” using the Actions tab in the Device Action Log Criteria node.

Exporting to XML
For exporting to XML, configure the directory and filename to which you want to send qualified logs in XML format. NetScreen-Security Manager uses this information when exporting qualified log entries to XML; each log becomes an XML record, which you can open in most Web browsers.

This setting simply defines the XML settings for the management system. To actually export logs to XML, you must select “XML Enable” using the Actions tab in the Device Action Log Criteria node.

Exporting to Email
For exporting to email, configure the following email and SMTP settings:

- SMTP Server—The server IP address that the SMTP server uses to send email.
- Default ‘From’ Email Address—Some SMTP servers require a valid “from” email address to relay mail.
- Default ‘To’ Email Addresses—The email address that receives email alarms. You can specify multiple “to” email addresses.

NetScreen-Security Manager uses this information when exporting qualified log entries to email. This setting simply defines the email and SMTP settings for the management system.

NOTE: After editing your email settings, you must restart the Device Server for your changes to take effect.

To actually export logs to email, you must select “SMTP Enable” using the Actions tab in the Device Action Log Criteria node.

NOTE: The email export settings in the Actions tab define the default email and SMTP settings for the management system. To export logs to email based on the log criteria, you can define From and To email addresses in the Device Action Log Criteria. However, if you select “SMTP Enable” within a Device Action Log Criteria instance but do not specify From and To email addresses in the instance, the management system automatically uses the default email settings (as defined in the Actions tab).
Setting Device Action Log Criteria

A Device Action Log Criteria instance defines the criteria for a qualified log; each instance contains two criteria settings (category and severity), and multiple action settings for logs that meet the criteria settings. For example, to only export critical severity attack logs to XML, you create a device action log criteria instance that specifies the log category as predefined, the severity as critical, and the action as XML. For each log entry that matches the criteria, NetScreen-Security Manager exports the log as XML, using the default XML settings configured in the Actions tab.

To add a new Device Action Log Criteria instance, use the Add button, then configure the following settings.

Selecting Category

In the Category list, select a category of log entry for the criteria. Some categories contain subcategories; however, to set an action based on a subcategory, you must first select a category.

For details on each category and subcategory, see Appendix D, “Log Entries”.

Selecting Severity

In the Severity tab, select the severities for the criteria.

Selecting Actions

In the Actions tab, select the actions (SNMP, syslog, XML, CSV, Email, and Script) you want the management system to take for logs that meet the criteria. You can enable multiple actions.

When you enable the Email/SMTP and Script actions, you can also configure the following additional settings:

- **Email Action**—To direct the management system to email qualified log records to a Simple Mail Transfer Protocol (SMTP) email file on the SMTP server, specify the From and To email addresses:
  - **From Email Address**—The email address that the SMTP server uses to send email. Some SMTP servers require a valid “from” email address to relay mail.
  - **To Email Addresses**—The email address that receives email alarms. You can specify multiple “to” email addresses.

  Configuring these settings overrides the default email addresses configured in the Actions tab. However, if you select “SMTP Enable” within a Device Action Log Criteria instance but do not specify From and To email addresses in the instance, the management system automatically uses the default email settings (as defined in the Actions tab).

- **Script Action**—To direct the management system to send qualified log records to a script, you must configure the following:
  - **Script Enable**
Script To Run—Select the script you want to run from the Script To Run list. For a script to appear in the list, the script must be located in the /usr/netscreen/DevSvr/var/scripts/ directory on the NetScreen-Security Manager Device Server. By default, this directory contains two sample scripts, sample.sh and sample.pl.

Action Upon Script Failure—Specify the error handling for the script:
- Skip. Directs the system to skip any log for which the script had an error.
- Retry. Directs the system to try the action again for the same log. When using this filter, you must also specify:
  - Retry Count. Specifies the maximum number of retries to attempt before moving on to the next log record.
  - Retry Interval (in seconds). Specifies the number of seconds until the action is tried again.

Using the Log2Action Utility to Export Logs
You can also use a command line utility on the Device Server to export logs. To export to XML, CSV, SNMP, Syslog, email, or script format using the Log2Action utility:

1. Log in to the NetScreen-Security Manager Device Server as root.
2. Change to the utility directory by typing: cd /usr/netscreen/DevSvr/utils
3. Specify the common filters, format, and format-specific filters for the format you want to export to:
   sh devSvrCli.sh --log2action <common_filters> --action <format> <format_options>

The log2action utility exports all log records to the specified format. After executing the action, the system generates an exit status code of 0 (no errors) or 1 (errors).

The following sections detail common filters, actions, and required and optional format-specific filters.

Using Filters
The log2action utility generates data for a maximum of 100,000 logs. Because of this, it is highly recommended that you specify filtering criteria when using the log2action utility. Without filtering, the action report generates data from the earliest date in the log database and stops providing output after 100,000 logs. In this case, it is possible that you may not get the action output of your most recent data. Specifying a time filter is recommended in this situation.

Using Time Filters
For example, if you wanted to view data in the logs of 20060317, run the following command:
If you wanted to view data for all logs from 20060315 to 20060317, run the following command:

```
./devSvrCli.sh -log2action -filter -log-id 20060315:0-20060317:4294967294
-action --xml --file-path /tmp/newtest.xml
```

Using Common Filters

To control which log records are exported, use common filters. Common filters are optional and must be used before the action command (`--action`).

To see all available common filters, type:

```
sh devSvrCli.sh --log2action --action
```

The following common filters display:

<table>
<thead>
<tr>
<th>Option</th>
<th>Default</th>
<th>Multiple</th>
<th>Specifies</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>--help</td>
<td>none</td>
<td>no</td>
<td>Prints this help message</td>
<td></td>
</tr>
<tr>
<td>--domain</td>
<td>*</td>
<td>yes</td>
<td>Domain path &lt;global[/&lt;subdomain-name&gt;]</td>
<td></td>
</tr>
<tr>
<td>--src-ip</td>
<td>*</td>
<td>yes</td>
<td>Source IP address &lt;a.b.c.d[/n</td>
<td>&lt;a.b.c.d] &gt;</td>
</tr>
<tr>
<td>--dst-ip</td>
<td>*</td>
<td>yes</td>
<td>Destination IP address &lt;a.b.c.d[/n</td>
<td>&lt;a.b.c.d] &gt;</td>
</tr>
<tr>
<td>--src-port</td>
<td>*</td>
<td>yes</td>
<td>Source port &lt;[0-65535][0-65535]&gt;</td>
<td></td>
</tr>
<tr>
<td>--dst-port</td>
<td>*</td>
<td>yes</td>
<td>Destination port &lt;[0-65535][0-65535]&gt;</td>
<td></td>
</tr>
<tr>
<td>--matches-to-return</td>
<td>no</td>
<td></td>
<td>Number of log entries to match &lt;[1-100000]&gt;</td>
<td></td>
</tr>
<tr>
<td>--log-id</td>
<td>*</td>
<td>no</td>
<td>From Log ID to To Log ID &lt; yyyyymmdd&gt;:&lt;0-MAX]</td>
<td>&lt; yyyyymmdd&gt;:&lt;0-MAX&gt;&gt;</td>
</tr>
<tr>
<td>--time_recv</td>
<td>*</td>
<td>yes</td>
<td>Time received &lt; yyyyymmdd&gt;:&lt;hhmss&gt;:&lt; yyyyymmdd&gt;:&lt;hhmss&gt;</td>
<td></td>
</tr>
<tr>
<td>--severity</td>
<td>*</td>
<td>yes</td>
<td>Severity &lt; none, info, warning, minor, major, critical)</td>
<td></td>
</tr>
<tr>
<td>--user-flag</td>
<td>no</td>
<td>yes</td>
<td>User flag number &lt; [0-7]&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>High = 0</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Medium = 1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Low = 2</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Closed = 3</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>False Positive = 4</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Assigned = 5</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Investigate = 6</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Follow-Up = 7</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Pending = 8</td>
<td></td>
</tr>
</tbody>
</table>
Some common filters support multiple entries, enabling you to specify more than one criteria. When using multiple entries for a common filter, you must use the common filter before each entry.

**Using Format-Specific Filters**

To control how log records are exported, use format-specific filters. Some formats have required and optional format-specific filters.

---

**NOTE:** Variable data is only exported in .csv format.

Use format-specific filters after the specified action. To see all format-specific filters for a format, type:

```
sh devSvrCli.sh --log2action --action --format
```

---

**Exporting to XML**

The xml action directs the system to output logs using the XML format. To export:

1. Login to the Device Server as root, then change to the utility directory by typing: `cd /usr/netscreen/DevSvr/utils`.

2. To export to a file, type:

```
sh devSvrCli.sh --log2action --action --xml <file-path> --include-header
```

The Device Server exports all log records to XML; each log record becomes an XML record, which you can open in most Web browsers.

---

**Using XML Required/Optional Format-Specific Filters**

You can use the following required and optional format-specific filters for exporting to XML:

<table>
<thead>
<tr>
<th>Option</th>
<th>Default</th>
<th>Multiple</th>
<th>Specifies</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>--rule</td>
<td></td>
<td></td>
<td>Rule to match</td>
<td>`&lt;domain-path&gt;:&lt;policy-name&gt;:&lt;rulebase (fw</td>
</tr>
<tr>
<td>--category</td>
<td>*</td>
<td>yes</td>
<td>Category</td>
<td><code>&lt;category&gt;</code>&lt;br&gt;(self, config, traffic, alarm, info, predefined, custom, screen, implicit)</td>
</tr>
<tr>
<td>--action</td>
<td>*</td>
<td>no</td>
<td>Action, usually followed by format-specific filters</td>
<td><code>&lt;action&gt;</code>&lt;br&gt;(csv, email, script, snmp, sylog, xml)</td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>Option</th>
<th>Default</th>
<th>Multiple</th>
<th>Required</th>
<th>What It Means</th>
</tr>
</thead>
<tbody>
<tr>
<td>--file-path</td>
<td>No</td>
<td>Yes</td>
<td></td>
<td>Specifies where the system should direct the output. For example, myLogs.xml</td>
</tr>
<tr>
<td>--include-header</td>
<td>No</td>
<td>No</td>
<td></td>
<td>Specifies that the system should print the field name before each field.</td>
</tr>
</tbody>
</table>
Viewing XML Format Output
To view the XML schema file, type:

```
/usr/netscreen/DevSvr/lib/logActions/log.xsd
```

**EXAMPLE: EXPORTING ATTACK CATEGORY LOG RECORDS TO XML**
To export predefined and custom attack category log records to an XML file located in the /usr directory of the Device Server, use the `--category` common filter to specify the categories:

```
sh devSrvcI.sh --log2action --category predefined
--category custom --action --xml --file-path
/usr/MyXmlLogRecords/attacks.xml
```

Exporting to CSV
The csv action directs the system to output logs using the CSV format. To export:

1. Login to the Device Server as root, then change to the utility directory by typing:
   
   ```
   cd /usr/netscreen/DevSvr/utils
   ```

2. To export to a file, type:

   ```
   sh devSrvcI.sh --log2action --action --csv <file-path>
   <include-header>
   ```

The Device Server exports all log records to CSV; each log record becomes an CSV record.

Using CSV Required/Optional Format-Specify Filters
You can use the following required and optional format-specific filters for exporting to CSV:

<table>
<thead>
<tr>
<th>CSV</th>
<th>Multiple</th>
<th>Required</th>
<th>What It Means</th>
</tr>
</thead>
<tbody>
<tr>
<td>--file-path</td>
<td>No</td>
<td>Yes</td>
<td>Specifies where the system should direct the output. For example, myLogs.csv</td>
</tr>
<tr>
<td>--include-header</td>
<td>No</td>
<td>No</td>
<td>Specifies that the system should print the field name before each field.</td>
</tr>
</tbody>
</table>

Viewing CSV Format Output
CSV log files use this format:

Day Id,Record Id,Time Received GMT, Time Generated GMT, Origin IP, Source IP, Source Port, Destination IP, Destination Port, User, Inbound Interface, Outbound Interface, Origin, Virtual Device, Attack, Policy Name, Policy Version, Rulebase, Rule Number, Misc, Comment, Bytes, Packets, Elapsed, Protocol, User Flag, Category, Sub Category, Is Hidden, Is Duplicate, Is Alert, Severity, Run Script, Send Email, Send SNMP Trap, Send Syslog, From External, Action, Variable Data
EXAMPLE: EXPORTING COLUMN HEADERS TO CSV
To print the column headers for log records when exporting to a CSV file, use the include-header option:

```
sh devSvrCl.sh --log2action --action --csv --include-header --file-path /usr/MyCSVLogRecords/logrecords.csv
```

Exporting to SNMP
The snmp action directs the system to output logs to an snmp server in snmp format. You must specify the SNMP community string and the SNMP server IP address that receives the exported log records.

To export:
1. Login to the Device Server as root, then change to the utility directory by typing: `cd /usr/netscreen/DevSvr/utils`
2. To export to a file, type:
```
sh devSvrCl.sh --log2action --action --snmp <community> <server>
```

The Device Server exports all log records to the specified SNMP community and server.

Using SNMP Required/Optional Format-Specify Filters
You can use the following required format-specific filters for exporting to SNMP:

<table>
<thead>
<tr>
<th>SNMP</th>
<th>Multiple</th>
<th>Required</th>
<th>What It Means</th>
</tr>
</thead>
<tbody>
<tr>
<td>--community</td>
<td>No</td>
<td>Yes</td>
<td>Specify SNMP community string. For details on the community parameter, refer to section 3.2.5 of RFC 1098 for. You might need to ask your SNMP server administrator for the server community string.</td>
</tr>
<tr>
<td>--server</td>
<td>No</td>
<td>Yes</td>
<td>Specify SNMP manager IP address</td>
</tr>
</tbody>
</table>

The SNMP format has no optional format-specific filters.

Viewing SNMP Format Output
SNMP trap log entries use the following format:

```
<day id>-<record id> <timestamp> <sensor addr> <src addr>:<src port> <dst addr>:<dst port> <nat src addr>:<nat src port> <nat dst addr>:<nat dst port> <user> <in nic> <out nic> <sensor vin> <virtual dev> <attack> <policy name>:<policy ver> <rulebase> <rule number> <bytes> <packets> <elapsed> <protocol> <category>-<subcategory> <action> <session id1>-<session id2> <is hidden> <is duplicate> <is alert> <severity> <run script> <send email> <send snmp> <send syslog>
```

EXAMPLE: EXPORTING TO A SNMP SERVER
To send log records to the public SNMP server at 192.168.1.15, use the --public and --server options:
```
sh devSvrCli.sh --log2action --action --snmp --community public --server 192.168.1.15
```

Exporting to Email

The email action directs the system to output logs to an email address in SMTP format. You must specify the recipient email address that receives the exported log records and, optionally, the sender email address.

To export:

1. Login to the Device Server as root, then change to the utility directory by typing: `cd /usr/netscreen/DevSvr/utils`
2. To export to a file, type:

   ```
   sh devSvrCli.sh --log2action --action --email <sender> <recipient>
   ```

   The Device Server exports all log records to the specified email address for the recipient.

   **NOTE:** You do not specify the SMTP server IP address in the log2action utility. The system uses the IP address configured for email in the Log Actions area of the GUI Server (in the NetScreen-Security Manager UI). For details on configuring this value, see “Exporting to Email” on page 771. You must configure the IP address before attempting to export logs to an email address.

Using Email Required/Optional Format-Specify Filters

You can use the following required and optional format-specific filters for exporting to email:

<table>
<thead>
<tr>
<th>Email/SMTP</th>
<th>Multiple</th>
<th>Required</th>
<th>What It Means</th>
</tr>
</thead>
<tbody>
<tr>
<td>--recipient</td>
<td>Yes</td>
<td>Yes</td>
<td>Specify the receiving email address for the SMTP log records</td>
</tr>
<tr>
<td>--sender</td>
<td>No</td>
<td>No</td>
<td>Specify the sender email address</td>
</tr>
</tbody>
</table>

Exporting to syslog

The syslog action directs the system to output logs to a syslog server in syslog format. You must specify the IP address of the syslog server that receives the exported log records and the syslog facility.

To export:

1. Login to the Device Server as root, then change to the utility directory by typing: `cd /usr/netscreen/DevSvr/utils`
2. To export to a file, type:

   ```
   sh devSvrCli.sh --log2action --action --syslog <server> <facility>
   ```
The Device Server exports all log records to the specified IP address for the syslog server.

Using Syslog Required/Optional Format-Specify Filters
You can use the following required format-specific filters for exporting to syslog:

<table>
<thead>
<tr>
<th>Syslog</th>
<th>Multiple</th>
<th>Required</th>
<th>What It Means</th>
</tr>
</thead>
<tbody>
<tr>
<td>--server</td>
<td>No</td>
<td>Yes</td>
<td>Specify syslog server IP address as [IP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>■ 192.168.1.25:7889</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>■ <a href="mailto:syslog.server@mycompany.com">syslog.server@mycompany.com</a>:7889</td>
</tr>
</tbody>
</table>
| --facility      | Yes      | Yes      | Specifies the facility that receives syslog messages. For details on the facility parameter, refer to section 4.1.1 of RFC 3164. The syslog severity, also used to calculate the overall syslog message priority, is automatically set to alert.

The syslog format has no optional format-specific filters.

Viewing Syslog Format Output
Syslog messages use the following format:

<day id>-<record id> <timestamp> <sensor addr>:<src port> <dst addr>:<dst port> <nat src addr>:<nat src port> <nat dst addr>:<nat dst port> <user> <in nic> <out nic> <sensor vin> <virtual dev> <attack> <policy name>:<policy ver> <rulebase> <rule number> <bytes> <packets> <elapsed> <protocol> <category>-<subcategory> <action> <session id1>-<session id2> <is hidden> <is duplicate> <is alert> <severity> <run script> <send email> <send smtp> <send syslog>

Exporting to a Script
The script action directs the system to execute a script, use STDIN to pass log records formatted as XML to the script, and report output status. You must specify the name of the script that receives the exported log records (script must be located in the /usr/netscreen/DevSvr/var/scripts/ directory).

To export:

1. Login to the Device Server as root, then change to the utility directory by typing: cd /usr/netscreen/DevSvr/utils.

2. To export to a file, type:

   sh devSvrCl.sh --log2action --action --script <script-name> <error-handling>

   The Device Server exports all log records to the specified script.
Using Script Required/Optional Format-Specify Filters

You can use the following required format-specific filters for exporting to a script:

<table>
<thead>
<tr>
<th>Script</th>
<th>Multiple</th>
<th>Required</th>
<th>What It Means</th>
</tr>
</thead>
<tbody>
<tr>
<td>--script-name</td>
<td>No</td>
<td>Yes</td>
<td>Specify script name. The script must be located in the /usr/netscreen/DevSvr/var/scripts/ directory.</td>
</tr>
<tr>
<td>--error-handling</td>
<td>No</td>
<td>Yes</td>
<td>Specifies error handling for the specified script. When using this filter, you must specify one of the following error-handling filters:</td>
</tr>
</tbody>
</table>
|                 |          |          | • --skip
|                 |          |          |    Directs the system to skip any log for which the script had an error. |
|                 |          |          | • --retry
|                 |          |          |    Directs the system to try the action again for the same log. When using this filter, you must also specify: |
|                 |          |          |    • --retry-interval
|                 |          |          |        Specifies the number of seconds until the action is tried again. |
|                 |          |          |    • --num-retries
|                 |          |          |        Specifies the maximum number of retries to attempt before moving on to the next log record. |

The script format has no optional format-specific filters.
Chapter 13
Reporting

Use the Report Manager module in Juniper Networks NetScreen-Security Manager to generate and view reports summarizing log and alarms generated by the managed Juniper Networks security devices in your network. You can use these reports to track and analyze log incidents, network traffic and potential attacks.

The following sections are in this chapter:

- About Reporting
- Report Types
- Setting Report Options
- Log Viewer Integration
- Using Reports
- Using Statistical Reports
About Reporting

The Report Manager module in NetScreen-Security Manager is a powerful and easy-to-use tool that enables you to generate reports summarizing key log and alarm data originating from the managed devices in your network. The reports in Report Manager provide a useful complement to the monitoring and logging capabilities in NetScreen-Security Manager enabling you to track and analyze network traffic, activities, and potential attacks.

Report Manager contains the following benefits for generating reports:

- Report Type Groupings
- Graphical Data Representation
- Integration with Logs
- Central Access to Management Information

Report Type Groupings

The reports in Report Manager are grouped together according to the type of data they provide:

- FW/VPN—Series of reports summarizing log and alarm data generated by the managed security devices in your network.
- DI/IDP—Includes reports that provide data on deep inspection and intrusion detection and prevention attacks.
- Screen—Includes reports that provide data on Screen attacks detected by the firmware on the managed security devices in your network.
- Administrative—Includes reports specifically designed to help system administrators track and manage log incidents and security rules.
- My Reports—Includes all reports that you have saved or created as a custom report.
- Shared Reports—Includes all reports that you have saved or created that you want made accessible to others in a domain.

Grouping these reports by type enable administrators and operations staff interested in tracking and analyzing specific types of information need to work only within the group of reports that they need.

For details on each of the specific reports per group, see “Report Types” on page 783. For additional details on each report type grouping, refer to the NetScreen-Security Manager Online Help.
Graphical Data Representation

You can use reports to view log data in both tabular and graphical form. The various depictions of the data make it easier to identify trends and potential areas of risk. Depending on your preference, you can also choose to view the data in either a horizontal bar graph or a pie chart.

Integration with Logs

Reports are also integrated with the Log Viewer and Log Investigator modules. By simply clicking a data point depicted in a report, you can quickly drill down to access and view the specific log entries presented in the report data. Refer to “Log Viewer Integration” on page 793 for more information on how you can use reports and log entries together to further analyze network events and attacks.

Central Access to Management Information

For network administrators and security analysts interested in tracking and identifying potential network trends and attacks, Report Manager provides a single, graphical view into the network.

Report Types

Report Manager contains two top-level categories:

- Predefined Reports on page 783
- My Reports on page 786

It is recommended that you use the pre-defined reports first to familiarize yourself with how reporting works in NetScreen-Security Manager. You can then later fine-tune these reports by generating custom reports based on them.

Predefined Reports

There are 32 pre-defined reports in Report Manager. Many of these reports provide a summary of key log events and alarms generated by the sensor(s) in your network (such as Top Scan Sources or Top Attacks). Two reports (Logs By User-set Flag and Top Rules) provide administrative information useful if you are tracking incidents or optimizing your rules. For typical use cases describing each of these reports, see Using Reports on page 795.

For your convenience, Report Manager group reports into the following categories:

- FW/VPN Reports
- DI/IDP Reports
- Screen Reports
- Administrative Reports
**FW/VPN Reports**

The following table lists and describes reports in NetScreen-Security Manager that provide information related to your network’s firewalls and VPNs.

**Table 75: Firewall and VPN Reports**

<table>
<thead>
<tr>
<th>Report</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Alarms</td>
<td>The total number of alarms generated by the managed security devices in your network, excluding traffic alarms.</td>
</tr>
<tr>
<td>Top Traffic Alarms</td>
<td>The total number of traffic alarms generated by the managed security devices in your network.</td>
</tr>
<tr>
<td>Top Traffic Log</td>
<td>The total number of traffic log entries generated by the managed security devices in your network, within filter constraints.</td>
</tr>
<tr>
<td>Top Configuration Logs</td>
<td>The total number of configuration log entries generated by the managed security devices in your network, within filter constraints.</td>
</tr>
<tr>
<td>Top Information Logs</td>
<td>The total number of information log entries generated by the managed security devices in your network, within filter constraints.</td>
</tr>
<tr>
<td>Top Self Logs</td>
<td>The total number of Self log entries generated by the managed security devices in your network, within filter constraints.</td>
</tr>
</tbody>
</table>

**DI/IDP Reports**

The following table lists and describes reports in NetScreen-Security Manager that provide deep inspection and intrusion detection and prevention information.

**Table 76: DI/IDP Reports**

<table>
<thead>
<tr>
<th>Report</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top 100 Attacks (last 24 hours)</td>
<td>those attacks that are detected most frequently within the last 24 hours.</td>
</tr>
<tr>
<td>Top 100 Attacks Prevented (last 24 hours)</td>
<td>those attacks that are prevented most frequently within the last 24 hours.</td>
</tr>
<tr>
<td>Top 20 Attackers (All Attacks - last 24 hours)</td>
<td>20 IP addresses that have most frequently been the source of an attack during the last 24 hours.</td>
</tr>
<tr>
<td>Top 20 Attackers Prevented (All Attacks - last 24 hours)</td>
<td>20 IP addresses that have most frequently been prevented from attacking the network during the last 24 hours.</td>
</tr>
<tr>
<td>Top 20 Targets (last 24 hours)</td>
<td>20 IP addresses that have most frequently been the target of an attack during the last 24 hours.</td>
</tr>
<tr>
<td>Top 20 Targets Prevented (last 24 hours)</td>
<td>20 IP addresses that have most frequently prevented attacks during the last 24 hours.</td>
</tr>
<tr>
<td>All Attacks by Severity (last 24 hours)</td>
<td>number of attacks by severity level (set in attack objects).</td>
</tr>
<tr>
<td>All Attacks Prevented by Severity (last 24 hours)</td>
<td>number of attacks by severity level (set in attack objects).</td>
</tr>
<tr>
<td>All Attacks Over Time (last 7 days)</td>
<td>all attacks detected during the last 7 days.</td>
</tr>
<tr>
<td>All Attacks Prevented Over Time (last 7 days)</td>
<td>all attacks prevented during the last 7 days.</td>
</tr>
<tr>
<td>All Attacks Over Time (last 30 days)</td>
<td>all attacks detected during the last 30 days.</td>
</tr>
</tbody>
</table>
Chapter 13: Reporting

Screen Reports
When the firmware on your device identifies an attack, it generates a log event. These events are totalled and summarized for your review in the following reports.

Table 77: Screen Reports

<table>
<thead>
<tr>
<th>Report</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Attacks Prevented Over Time (last 30 days)</td>
<td>all attacks prevented during the last 30 days.</td>
</tr>
<tr>
<td>Critical Attacks (last 24 hours)</td>
<td>all attacks categorized as “critical” detected during the past 24 hours.</td>
</tr>
<tr>
<td>Critical Attacks Prevented (last 24 hours)</td>
<td>all attacks categorized as “critical” prevented during the past 24 hours.</td>
</tr>
<tr>
<td>Critical Thru Medium Attacks (last 24 hours)</td>
<td>all attacks categorized as either “critical” or “medium” detected during the past 24 hours.</td>
</tr>
<tr>
<td>Critical Thru Medium Attacks Prevented (last 24 hours)</td>
<td>all attacks categorized as either “critical” or “medium” prevented during the past 24 hours.</td>
</tr>
<tr>
<td>Top 50 Scan Sources (last 7 days)</td>
<td>50 IP addresses that have most frequently performed a scan of a managed device</td>
</tr>
<tr>
<td>Top 50 Scan Targets (last 7 days)</td>
<td>50 IP addresses that have most frequently been the target of a scan over the last 7 days.</td>
</tr>
<tr>
<td>Top IDP Rules</td>
<td>The total number of log entries generated by specific rules in your IDP policies. You can use the “Top Rules” report to identify those rules that are generating the most log events. This enables you to better optimize your rulebases by identifying those rules that are most and least effective. You can then modify or remove those rules from your Security Policies.</td>
</tr>
</tbody>
</table>

Administrative Reports
The following table lists and describes reports in NetScreen-Security Manager that provide information specifically for administrators:
Table 78: Administrative Reports

<table>
<thead>
<tr>
<th>Report</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logs by User-set Flag</td>
<td>The total number of log entries that were flagged by an administrator in the Log Viewer according to the predefined flag type set. You can flag log events as either High, Medium, Low, Closed, False Positive, Assigned, Investigate, Follow-Up, or Pending. You can use the “Logs by User-set Flag” report to quickly identify log events of specific interest.</td>
</tr>
<tr>
<td>Top Rules</td>
<td>The total number of log entries generated by specific rules in your ScreenOS/DI policies. You can use the “Top Rules” report to identify those rules that are generating the most log events. This enables you to better optimize your rulebases by identifying those rules that are most and least effective. You can then modify or remove those rules from your Security Policies.</td>
</tr>
</tbody>
</table>

For more specific information describing each report, refer to the NetScreen-Security Manager Online Help.

My Reports

Once you are comfortable using reports, you can create your own custom reports to provide the exact information that your network security needs require. My reports are associated with a specific user across domains.

Shared Reports

You can also allow others to use your custom reports by creating them as a “shared” report. Shared reports are associated with domains. Subject to user-defined access control settings, shared reports are available to all other users in the domain.

Working With Reports

Using the Report Manager, you can perform the following actions:

- Generating a Pre-Defined Report on page 786
- Creating a Custom Report on page 787
- Generating Reports Automatically on page 788
- Deleting Reports on page 790
- Exporting Reports to HTML on page 790

Generating a Pre-Defined Report

To generate a pre-defined report, simply click that report from the Report Manager. The report is generated according to its default report settings. You can set different report options to further tailor your reports to your specific needs. Refer to Setting Report Options on page 790 for more information.
Creating a Custom Report

You can also create your own custom report based on your own reporting requirements.

To create a custom report:


2. Use the General tab to configure report options. Refer to Setting Report Options on page 781 for more information.

3. Use the Log Filter tab to configure report filters. Refer to Modifying Report Filters on page 792 for more information.
4. Click OK when you are done.

The report now appears under the My Reports node.

You can also use an existing pre-defined report as the basis for a custom report by simply generating that report and renaming it.

For example, you are a security administrator responsible for monitoring and protecting the corporate DMZ network. You are overjoyed that a “Top Attacks” report comes pre-defined in IDP. The report however, displays attacks on the entire network, and you are interested only in the DMZ. You decide to create your own custom report:

1. In the Objects component, you configure a network object called “Corporate DMZ Network” and add all the IP addresses located in the DMZ.

2. Using the “Top Attacks” report, use Save As to rename the report “Top DMZ Attacks”. You can also click the Save As... icon on the toolbar or use the <Ctrl-S> keyboard shortcut.

3. In the Columns for Report, select Destination Address.

4. In the Log Filter tab, select to filter on only those destination addresses defined in the Corporate DMZ network object.

NetScreen-Security Manager creates the new report and displays it in the Navigation Tree under Custom Reports.

You can also use the same process to copy reports.

Generating Reports Automatically

You can also generate reports automatically using the Scheduled Log-Based Report utility, a command line utility located on the NetScreen-Security Manager GUI Server. The utility works with scripts enabling you to generate and then send the reports to you using email or ftp.

To generate reports automatically:

1. Log in to the NetScreen-Security Manager GUI Server as root.

2. Change to the utility directory by typing: cd /usr/netscreen/GuiSvr/utils

3. Specify the report(s) that you want to generate and the script that you want to use:

   sh guiSvrCli.sh --generate-reports --report "<report name>" --script <script>

When you specify the report, do so in the following format using the domain path and report name:
"""<domain-path>.<report-name>""

Specify the domain-path in the following format:

global[.<subdomain-name>]

**NOTE:** Use double quotation marks to enclose the domain path and report name.

When you specify the script, use the name of the script as it exists in the scripts directory (/usr/netscreen/GuiSvr/var/scripts).

For example, type the following command:

```
sh guiSvrCli.sh --generate-reports --report ""global.shared:schedreport"" --script ftp.sh
```

**NOTE:** Sample scripts enabling you to email and ftp the report results are available in /usr/netscreen/GuiSvr/lib/scripts for your convenience. To use these scripts, it is recommended that you first copy them to /usr/netscreen/GuiSvr/var/scripts, and then change the permissions on the scripts so that they are both writable and executable. You can then customize the scripts for your appropriate needs.

**NOTE:** The email.pl and emailReports.sh scripts only do MIME formatting of the reports. The actual mailing is done by sendmail or other Mail Transfer Agent (MTA). If you require authentication to send these reports, you must configure the authentication parameters as part of the MTA configuration. If you are using the ftp script to send you reports, you will also need to add values for the remote host, userid and password for the ftp account in the ftp.sh file.

The Scheduled Log-Based Report utility generates the report(s) and executes the script. You can view expanded report generation results using the Job Manager and Audit Log Viewer in the NetScreen-Security Manager UI, as detailed in the following sections.

### Using Cron with Scheduled Reports

Cron is the method used to schedule report tasks. The command “crontab -e” invokes a text editor (e.g., vi) enabling you to edit the “crontab” file. The crontab file consists of five fields specifying the time (0-23 for hour, 0-59 for minutes), specific date (1-12 for month, 0-31 for day; enter an asterisk * if you want to run the report everyday) and day of the week (1-7 with 1=Monday) that you wish to run scheduled report tasks.

For example if you wanted to generate a report every Monday at midnight, you would enter the following:

```
0 0 * * 1 export NSMUSER=global/<user name>; export NSMPASSWD=<password>; /usr/netscreen/GuiSvr/utils/guiSvrCli.sh --generate-reports --report ""global:system:Top Screen Attacks"" --script ftp.sh
```
Deleting Reports

If a custom report no longer serves your informational needs, you can delete it. Note however, that you cannot delete pre-defined reports.

To delete a custom report, select the custom report you want to delete and select Delete from the File menu. You can also right-click the report and select Delete, or use the Ctrl-D keyboard shortcut.

Exporting Reports to HTML

Once you are done creating your reports, you can then export them into HTML. For example, if you wanted to share information with other security experts about the attacks that you are noticing in your network, you could use the following process to export the report onto disk:

1. Select Export Reports from the File menu. Alternatively, you could right-click in the chart window, and use the “Export reports in HTML” option. The Export Reports window appears.

2. Check the Top Attacks report checkbox.

3. Click Browse to save the file onto CD or to any other location on your desktop.

4. Click Export. The report is exported onto your CD.

NetScreen-Security Manager saves the report in several file formats (such as .png, .html, and .gif) that you can later display in any web browser.

Setting Report Options

Each report in NetScreen-Security Manager provides information based on data available from the current day in a horizontal bar chart by default. You can configure the duration, number of data points, and graphical appearance of each report depending upon your preference by using the Set Report Options selection in the View menu.

NOTE: You can also access the Set Report Options dialog by right-clicking the chart on each report.

Use the Set Report Options selection in the View menu to tailor your reports to display only the specific information that you want. You can configure the following options in each report:

- report title
- report type
- columns for the report
- time period
- data point count
Setting Report Options

Chapter 13: Reporting

- chart type

You can also access the Set Report Options dialog by right-clicking the chart on each report.

Naming a Report

You can enter a name for a new report or rename an existing report in the General tab of the Set Report Options window. You can also configure the name of the report as displayed in the report graph by editing its Report Title.

Setting the Report Type

You can create two types of reports:

- Time Based - displays activity over time. Time-based reports for example, the Attacks Over Time report is a time-based report that measures the top attacks recorded in log records over a specified time period.

- Count Based - displays total current activity to date. Count-based reports for example, the Top Scan Targets report is a count-based report that displays the total number of scans currently recorded against a specified number of destination IP addresses.

Configuring Report Source Data

You can configure a report to one of the following log record columns: Action, Alert, Src Addr, or Policy. Select the report source data by checking the appropriate checkboxes in the Columns For Report selection area. The data that you choose for the columns in your report appear in the Y-axis of the graph.

Configuring a Report Time Period

You can configure a report to display all available data from either a specific date and time or during a specific time interval.

For example, if you had reason to suspect that your network was attacked on September 11 at 6:00pm, you could set the Starting At field in the Time Period Duration report options on a “Top Screen Attacks” report to that time, and generate the report.

If you were not sure of the exact date or time of the attack, but knew it occurred during the past 2 days, you could set the Duration field in the Time Period Duration report options on a “Top Screen Attacks” report to 2 days, and generate the report.

NOTE: The data that you can display in each report is limited by the amount of log information available.
Configuring the Data Point Count

Typically, the top fifty occurrences of each data type are displayed in each report. You can configure a report to display more or less data points depending upon the level of detail you need. For example, if you want to obtain a more precise view of the top occurrences of events, you would configure a lower Data Point Count (such as 25).

NOTE: The minimum data point count that you can configure in all reports is 5; the maximum data point count is 200.

Configuring the Chart Type

Each report depicts information in a horizontal bar chart by default. You can also configure the report to depict information using a pie chart.

Sharing Your Custom Report

Use the Save Report In pull-down menu and select the Shared Reports option to specify that you want to share your report across all domains.

Modifying Report Filters

You can also use report filters to reduce the amount of unwanted or unnecessary log information compiled in each report. This makes it easier for you to focus on only the log data of interest to you. You can specify criteria to filter your log data on any of the columns that you have chosen to base the report.

For example, you are a security administrator that typically reviews the “Attacks by Severity” report. You notice that critical attacks are on the rise. To track this more closely, you can modify the log filter on the “Attacks by Severity” report so that the report only displays critical attacks. To do this, you would select the “Attacks by Severity” report, and use Set Report Options to access the Log Filter tab. In the Log Filter tab, you would select to filter on attacks, and unselect all attacks except for those that are critical.

Configuring Report Processing Warnings

Each time you generate a report, it must perform a scan operation on a certain set of log records in the log database. The total number of log records that a report operation requires can have an adverse impact on your overall management performance. To prevent extraordinarily “lengthy” report operations from impacting your overall system performance, you can use the Preferences tool to configure NetScreen-Security Manager to display a warning message before a report is to scan a certain threshold number of log records.

This setting also applies to the Dashboard and Log Investigator.

For example, if you did not want any reports to interfere with the overall management performance, you would want to set a warning message threshold at around 1,000,000 logs. To do this you would use the Preferences option in the Tools menu and select Reports. In the New Preference Settings dialog box, click in the “Enable Warnings” checkbox and use the up and down arrows to specify 1,000,000 as the number of Maximum Records to Filter.
Once this preference is applied, a warning appears each time a report is set to perform an operation requiring 1,000,000 log records to be scanned.

**Saving Your Report Settings**

Once you have defined your custom reports, you can save the report settings as a custom report. Saved reports are organized under the tree node named “Custom Reports”.

**Log Viewer Integration**

Report Manager uses log data as the basis of all the information presented in each report. Because of this, it is recommended that you consider requirements for reporting as you decide how many log entries you want to maintain and store.

**Viewing Logs From Report Manager**

One key benefit of Report Manager’s tight integration with log entries is the ability to quickly access the source log data presented in each report. To view the source log entries in the Log Viewer for more detailed information about the report data, simply right-click a data point in any report and select Log Viewer from the View menu. The source log entries will appear in the Log Viewer.

---

**NOTE:** You cannot save the view generated in the Log Viewer for use in a later UI session.
Generating Quick Reports

Similarly, you can generate a Quick Report from data that appears in the Log Viewer or Log Investigator. Use the Quick Report tab located at the bottom of the Log Viewer or Log Investigator, and a count-based custom report called a Quick Report appears.
Using Reports

The following examples describe typical use cases for the reports in NetScreen-Security Manager.

EXAMPLE: USING ADMINISTRATIVE REPORTS TO TRACK INCIDENTS

In this example, firewall administrators are using the Log Viewer to monitor and investigate log events. They are specifically interested in configuration changes that are causing outages sporadically throughout the network. When they encounter a configuration log that seems out of the ordinary, they are flagging the log using the pre-defined flag type "Investigate".
After completing their investigation, they change the flag to either “Closed” or “Assigned” for further investigation. During normal operations, firewall administrators are investigating over 200 log entries per day.

You are a network manager interested in the progress of the investigation. To help track the progress, you generate a “Logs by User-set Flag” report.

By setting the duration of the report to 1 week, you can determine the total number of log entries flagged for investigation, total closed, and total assigned for further analysis.
EXAMPLE: USING ADMINISTRATIVE REPORTS TO OPTIMIZE RULEBASES

In this example, you are a security administrator responsible for implementing new rules to your firewall rulebase. After you have updated the new Security Policy on the managed security devices in your network, you are interested in knowing the effect of the new rules on network traffic.

You configure a “Top Rules” report to start at the same date and time that the new rulebase settings were updated in the network. You also set the report data point count to 100. In this way, you can get an indication for the top 100 rules that are generating log events.
By identifying the new rules that you implemented in the network, you can track how effective the new rules are. If you find that a specific rule that is permitting too much traffic, you may want to redefine it to be more strict. If you find that a specific rule is not generating any log events, you may want to check it again to verify that you configured it correctly; perhaps you configured an IP address incorrectly.

Regular review of the “Top Rules” report can help you to update and optimize the rulebases implemented in your Security Policies.

EXAMPLE: USING FW/VPN REPORT TO TRACK CONFIGURATION CHANGES
In this example, you are a firewall administrator responsible for configuring all the managed security devices in your network. You routinely update your network configurations after hours. To verify that your changes are taking effect, you routinely generate a “Top Configuration Logs” report each night at 1:00am.

During the day, you can generate a similar report to track any unauthorized configuration changes to your security devices.
In this example, you are a security administrator in the network operations center responsible for tracking potential network attacks. You routinely generate and track an “Attacks By Severity” report daily.

Over time, you notice that the number of critical attacks has increased 20%. To verify this, you can also generate a “Attacks over Time” report for the past 30 days.

The report indicates a recent increase in attacks as detected by your firewall. You can generate “Top Attacks”, “Top Attackers”, and “Top Targets” reports to further investigate the nature and assess the risk of these attacks.

For details on generating and configuring these reports, refer to the NetScreen-Security Manager Online Help.

EXAMPLE: USING DI REPORTS TO DETECT APPLICATION ATTACKS

In this example, you are a security analyst responsible for tracking potential deep inspection attacks. You routinely generate an “Attacks By Severity” report daily to track and identify potential attacks.

One day, you notice a significant increase in the number of critical attacks as detected by the deep inspection rules you have implemented in your Security Policy. You then generate a “Top Attackers” report for the last day.
The report indicates an IP Address as the top attacker for all the deep inspection attacks that you have been tracking. You recognize the IP address as an external server that is running a service using a non-standard protocol. Although the traffic is not malicious, it happens to match a malicious signature anomaly that you have configured in your deep inspection policy. You can then revise your policy rules to reclassify this traffic.

For details on generating and configuring these reports, refer to the NetScreen-Security Manager Online Help.

### Using Statistical Reports

If you previously used Historical Reports in NetScreen-Global PRO, and you wish to continue to generate reports using historical data, it is highly recommended that you install the NetScreen-Statistical Report Server with NetScreen-Security Manager. Refer to the NetScreen-Statistical Report Server Installer’s Guide and NetScreen-Statistical Report Server Administrator’ Guide for more information describing how to install and use the NetScreen-Statistical Report Server.

If you do not wish to install NetScreen-Statistical Report Server, you can continue to use your existing Historical Report Server as part of your NetScreen-Security Manager implementation.

Refer to the NetScreen-Security Manager 2004 FP2 Migration Guide for more information on maintaining your previous implementation of Historical Report Server with NetScreen-Security Manager. You can also refer to the NetScreen-Global PRO Report Manager User's Guide for more information on how to use historical reports.
The appendixes in Part 5 of the NetScreen-Security Manager 2005.3 Administrators Guide describe the terms used in this guide, listings of log entry categories and log entries, and other additional information you might find useful when using NetScreen-Security Manager.

Part 5 contains the following appendixes:

- Appendix A, Glossary defines terms and concepts used in the NetScreen-Security Manager environment.
- Appendix B, Unmanaged Commands details unsupported ScreenOS CLI commands.
- Appendix C, SurfControl URL Categories details the predefined URL categories provided and maintained by SurfControl.
- Appendix D, Log Entries details log entry categories and subcategories.
- Appendix E, Common Criteria EAL2 Compliance describes actions required for a security administrator to properly secure the NetScreen-Security Manager system and NetScreen-Security Manager User Interface to be in compliance with the Common Criteria EAL2 security target for Juniper Networks IDP 3.0 functionality.

For help in locating documentation for a term, task, or concept in this guide, see Part 6, “Index” on page 905.
Appendix A
Glossary

**Access List.** A list of network prefixes that are compared to a given route. If the route matches a network prefix defined in the access list, the route is either permitted or denied.

**Access-Challenge.** An additional condition required for a successful Telnet login by an authentication user via a RADIUS server.

**Action (Deep Inspection).** A DI action is performed by a security device when the permitted traffic matches the attack object specified in the rule. Deep Inspection actions include drop connection, drop packet, close client, and so on.

**Action (firewall).** A firewall action is performed by a security device when the device receives traffic that matches the direction, source, destination, and service. Firewall actions include permit, deny, reject.

**Activate Device Wizard.** The Activate Device wizard guides you through activating a modeled device in the NetScreen-Security Manager User Interface.

**Add Device Wizard.** The Add Device wizard guides you through importing or modeling a new device to the NetScreen-Security Manager User Interface.

**Address Object.** An address object represents a component of your network, such as a workstation, router, switch, subnetwork, or any other object that is connected to your network. Use address book objects to specify the network components you want to protect.

**Address Shifting.** A mechanism for creating a one-to-one mapping between any original address in one range of addresses and a specific translated address in a different range.

**Address Spoofing.** Address Spoofing is a technique for creating packets with a source IP address that is not the actual interface address. Attackers may use spoofed IP address to perform DDoS attacks while disguising their true address, or to take advantage of a trusted relationship between two hosts. To guard against spoofing attacks, configure a security device to check its own route table. If the IP address is not in the route table, the security device denies the traffic.

**Adjacencies.** When two routers can exchange routing information with one another, they are considered to have constructed an adjacency. Point-to-point networks have only two routers so those routers automatically form an adjacency. But point-to-multipoint networks are a series of several point-to-point networks. When routers pair in this more complex networking scheme, they are considered to be adjacent to one another.

**Advanced Encryption Standard (AES).** AES is a 128-bit encryption key standard. Use AES in your VPNs when you need greater interoperability with other network security devices.
Advertisement. A method a router uses to announce itself to other devices on the network, transmitting basic information including IP address, network mask, and other data.

Aggregate State. A router is in an aggregate state when it is one of multiple virtual BGP routing instances bundled into one address.

Aggregation. The process of combining several different routes in such a way that only a single route advertises itself. This technique minimizes the size of the routing table for the router.

Aggregator. An object used to bundle multiple routes under one common route generalized according to the value of the network mask.

Aggressive Aging. A mechanism to accelerate the timeout process when the number of sessions in the session table surpasses a specified high-watermark threshold. When the number of sessions in the table dips below a specified low-watermark threshold, the timeout process returns to normal.


APN. Access Point Name. An APN is an IE included in the header of a GTP packet that provides information on how to reach a network. It is composed of two elements: a network ID and an operator ID.

Application Layer Gateway (ALG). On a security device, an ALG is a software component that is designed to manage specific protocols such as SIP or FTP. The ALG intercepts and analyzes the specified traffic, allocates resources, and defines dynamic policies to permit the traffic to pass securely through the security device.

Area Border Router. A router with at least one interface in Area 0 and at least one interface in another area.

Area Range. A sequence of IP addresses defined by a lower limit and upper limit that indicates a series of addresses of devices that exist within an area.

Area. The most fundamental ordering method in the OSPF routing protocol. An OSPF area divides the internetwork into smaller, more manageable constituent pieces. This technique reduces the amount of information that each router must store and maintain about all the other routers. When a router in the area needs information about another device in or out of the area, it contacts a special router that stores this information. This router is called the Area Border Router (ABR) and contains all essential device information. In addition, the ABR area border router filters all information coming into the area to avoid bogging down other routers in the area with information they may not need.

AS Number. The identification number of the local autonomous system mapped to a BGP routing instance. The ID number can be any valid integer.

AS Path Access List. An access list used by a BGP routing instance to permit or deny packets sent by neighbor routing instances to the current virtual routing instance.

AS Path Attribute Class. The BGP provides four classes of path attributes. Well-Known Discretionary, Optional Transitive, and Optional Non-Transitive.

AS Path String. A string that acts as an identifier for an AS path. It is configured alongside an AS Path access list ID.

AS. See Autonomous System.
Atomic Aggregate. An object used by a BGP router to inform other BGP routers that the local system selected a generalized route.

Atomic Configuration. Atomic configuration is a fail-safe feature in ScreenOS 5.x. For devices running ScreenOS 5.x, if the configuration deployment fails for any reason, the device automatically uses the last installed stable configuration. Additionally, if the configuration deployment succeeds, but the device loses connectivity to the management system, the device rolls back to the last installed configuration. This minimizes downtime and ensures that NetScreen-Security Manager always maintains a stable connection to the managed device.

Attack Objects. An attack object contains attack patterns for known attacks that attackers can use to compromise your network. Use attack objects in your firewall rules to enable your security devices to detect known attacks and prevent malicious traffic from entering your network.

Attack Protection. Attack Protection is defined by the DI Profile used in a firewall rule.

Audit Log Target. An Audit Log Target is a directive that was sent to a security device.

Audit Log Viewer. The Audit Log Viewer is a module of the NetScreen-Security Manager User Interface. The Audit Log Viewer records administrative actions. Each audit log includes the date and time the administrative action occurred, the NetScreen-Security Manager admin who performed the action, and the domain (global or a subdomain) in which the action occurred.

Authentication Header (AH). See ESP/AH.

Authentication Server Objects. An authentication server provides authentication for NetScreen-Security Manager administrators and RAS users on your network. Use authentication servers objects to set a default authentication server for the global domain and each subdomain, or access an external RADIUS or SecurID system to provide authentication.

Authentication. Authentication ensures that digital data transmissions are delivered to the intended receiver. Authentication also assures the receiver of the integrity of the message and its source (where or whom it came from). The simplest form of authentication requires a user name and password to gain access to a particular account. Authentication protocols can also be based on secret-key encryption, such as DES, or on public-key systems using digital signatures.

Autonomous System (AS). An AS is a set of routers set off from the rest of the network and governed by a single technical administration. This router group uses an interior gateway protocol (IGP) or several IGPs and common metrics to route packets within the group. The group also uses an exterior gateway protocol (EGP) to route packets to other ASs. Each AS has a routing plan that indicates what destinations are reachable through it. This plan is called the Network Layer Reachability Information (NLRI) object. BGP routers generate and receive NLRI updates periodically.

Autonomous System Boundary Router. A router that connects an AS running one routing protocol to another AS running a different protocol.

Autonomous System Path. A list of all the autonomous systems that a router update has traveled through in the current transmission.

Bastion Host. A bastion host is a hardened system that is configured with the minimal software to support a single network service.

BGP Neighbor. (also known as a BGP Peer). BGP is a the Border Gateway Patrol dynamic routing protocol. A BGP neighbor is another device on the network that is running BGP.

Border Gateway Protocol (BGP). An inter-autonomous system routing protocol. BGP routers and autonomous systems exchange routing information for the Internet.
**Broadcast Network.** A network that connects many routers together and can send, or broadcast, a single physical message to all the attached routers. Pairs of routers on a broadcast network are assumed to be able to communicate with each other. Ethernet is an example of a broadcast network. On broadcast networks, the OSPF router dynamically detects its neighbor routers by sending Hello packets to the multicast address 224.0.0.5. For broadcast networks, the Hello protocol elects a Designated Router and Backup Designated Router for the network.

**CIDR (Classless Inter-Domain Routing).** An IP addressing scheme in which a single IP address is used to designate multiple unique IP addresses. A CIDR address includes an IP address and an IP network prefix.

![Figure 214: CIDR Translation](image)

<table>
<thead>
<tr>
<th>CIDR format</th>
<th>First host</th>
<th>Last host</th>
<th>Number of hosts</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.0.1/24</td>
<td>192.168.0.1</td>
<td>192.168.0.254</td>
<td>254</td>
</tr>
<tr>
<td>192.168.0.1/25</td>
<td>196.168.0.1</td>
<td>192.168.0.126</td>
<td>126</td>
</tr>
<tr>
<td>192.168.0.1/26</td>
<td>192.168.0.1</td>
<td>192.168.0.62</td>
<td>62</td>
</tr>
<tr>
<td>192.168.0.1/27</td>
<td>192.168.0.1</td>
<td>192.168.0.30</td>
<td>30</td>
</tr>
<tr>
<td>192.168.0.1/29</td>
<td>192.168.0.1</td>
<td>192.168.0.9</td>
<td>6</td>
</tr>
<tr>
<td>192.168.0.9/29</td>
<td>192.168.0.9</td>
<td>192.168.0.14</td>
<td>6</td>
</tr>
<tr>
<td>192.168.0.10/30</td>
<td>192.168.0.10</td>
<td>192.168.0.11</td>
<td>2</td>
</tr>
<tr>
<td>10.0.0.0/8</td>
<td>10.0.0.1</td>
<td>10.255.255.254</td>
<td>16777214</td>
</tr>
<tr>
<td>10.0.1.17/28</td>
<td>10.0.1.17</td>
<td>10.0.1.30</td>
<td>14</td>
</tr>
</tbody>
</table>

**Circuit-level Proxy.** Proxy or Proxy Server is a technique used to cache information on a Web server and acts as an intermediary between a Web client and that Web server. This proxy holds the most commonly and recently used content from the World Wide Web to provide quicker access to content for users and to increase server security.

**Classless Routing.** Support for interdomain routing, regardless of the size or class of the network. Network addresses are divided into three classes, but these are transparent in BGP, giving the network greater flexibility.

**CLI.** The CLI is the command line interface.

**Cluster List.** A list of paths recorded as a packet travels through a BGP route reflector cluster.

**Community.** A community is a grouping of BGP destination. By updating the community, you automatically update its member destinations with new attributes.

**Confederation.** An object inside a BGP AS that is a subset of routing instances in the AS. By grouping devices into confederations inside a BGP AS, you reduce the complexity associated with the matrix of routing connections, known as a mesh, within the AS.

**Configlet.** A configlet is a small, static configuration file that contains information on how a security device can connect to NetScreen-Security Manager.

**CRC Errors.** CRC errors indicate the number of packets generating a cyclic redundancy code error processed through the security device over the selected interface.
**Data Encryption Standard (DES).** DES is a 40- and 56-bit encryption algorithm developed by the National Institute of Standards and Technology (NIST). DES is a block encryption method originally developed by IBM. It has since been certified by the U.S. government for transmission of any data that is not classified top secret. DES uses an algorithm for private-key encryption.

**Data Encryption Standard-Cipher Block Chaining (DES-CBC).** DES-CBC is used to encrypt single DES keys.

**DCF.** See device capability file.

**Default Route.** A “catch all” routing table entry that defines the forwarding of traffic for destination networks that are not explicitly defined in the routing table. The destination network for the default route is represented by the network address 0.0.0.0/0.

**Delta.** A delta is a difference, or discrepancy. Example: the differences between the configuration running on the physical device and the difference between the configuration in NetScreen-Security Manager are known as deltas.

**De-Militarized Zone (DMZ).** A DMZ is an area between two networks that are controlled by different companies. A DMZ ethernet can be external or internal; external DMZ ethernets link regional networks with routers.

**Denial of Service (DoS) Attack.** A DoS attack is designed to disrupt a network service. Typically, an attacker sends a flood of information to overwhelm a service’s system resources, causing the server to ignore valid network requests. Other DoS attacks can cause the service process to crash.

**Device Administrator.** A device administrator is the person who uses WebUI or CLI to manage a single security device.

**Device Monitor.** The Device Monitor displays information about individual devices, their configuration and connection status, and memory usage.

**Device Server.** The Device Server is the component of the NetScreen-Security Manager management system that handles communication between the GUI Server and the device, collects data from the managed devices on your network, formats configuration information sent to your managed device, and consolidates log and event data.

**DHCP (Dynamic Host Configuration Protocol).** DHCP is used to dynamically assign IP addresses to networked computers.

**Directive.** A directive is a command send by NetScreen-Security Manager to your managed devices. Directives include importing, updating, rebooting, and so on. When you send a command to a device or group of devices, NetScreen-Security Manager creates a job for that command and displays information about that job in the Job Manager.

**Distributed Denial of Service (DDoS) Attack.** A DoS attack (typically a flood) from multiple source points. A DDoS attacks is more effective than a DoS attack, as it is no longer one computer against one server in an effort to overwhelm the server.

**DM (Data Model).** A Data Model is an XML file that contains configuration data for an individual device. The DM is stored in the Device Server; when you create, update, or import a device, the GUI Server edits the Abstract Data Model (ADM) to reflect the changes, then translates that information to the DM.

**DNS.** The Domain Name System maps domain names to IP addresses.

**Domain Menu.** The Domain Menu is the pull-down menu above the navigation tree where domains and subdomains are selected.
**Domains.** A domain is a logical grouping of devices, their policies, and their access privileges. A domain can contain devices, templates, objects, policies, VPNs, administrators, activities, authentication servers, groups—a representation of the all or a subset of the physical devices and functionality on your network. The domain above a domain is the parent domain, and the domain below a domain is the child domain. Domains at the same level are considered peer domains.

**Dynamic Routing.** A routing method which adjusts to changing network circumstances by analyzing incoming routing update messages. If the message indicates that a network change has occurred, the routing software recalculates routes and sends out new routing update messages. These messages populate the network, directing routers to rerun their algorithms and change their routing tables accordingly. There are two common forms of dynamic routing, including Distance Vector Routing and Link State Routing.

**Encryption.** Encryption is the process of changing data into a form that can be read only by the intended receiver. To decipher the message, the receiver of the encrypted data must have the proper decryption key. In traditional encryption schemes, the sender and the receiver use the same key to encrypt and decrypt data. Public-key encryption schemes use two keys: a public key, which anyone may use, and a corresponding private key, which is possessed only by the person who created it. With this method, anyone may send a message encrypted with the owner's public key, but only the owner has the private key necessary to decrypt it. PGP (Pretty Good Privacy) and DES (Data Encryption Standard) are two of the most popular public-key encryption schemes.

**Equal Cost Multipath.** Equal Cost MultiPath (ECMP) assists with load balancing among two to four routes to the same destination or increases the effective bandwidth usage among two or more destinations. When enabled, security devices use the statically defined routes or dynamically learn multiple routes to the same destination through a routing protocol. The security device assigns routes of equal cost in round robin fashion. Default: disabled

**ESP/AH.** AH and ESP are IP level security headers that were originally proposed by the Network Working Group focused on IP security mechanisms known as IPSec. The term IPSec refers to packets, keys, and routes associated with ESP and AH headers. The IP Authentication Header (AH) provides authentication. The IP Encapsulating Security Header (ESP) provides confidentiality to IP datagrams.

**Ethernet.** Ethernet is a local area network (LAN) technology invented at the Xerox Corporation, Palo Alto Research Center. Ethernet is a best-effort delivery system that uses CSMA/CD technology. Ethernet can be run over a variety of cable schemes, including thick coaxial, thin coaxial, twisted pair, and fiber optic cable. Ethernet is a standard for connecting computers into a local area network (LAN). The most common form of Ethernet is called 10BaseT, which denotes a peak transmission speed of 10 Mbps using copper twisted-pair cable.

**Export Rules.** When you have two or more virtual routers on a security device, you can configure export rules that define which routes on one virtual router are allowed to learned by another virtual router. See also Import Rules.

**External Neighbors.** Two BGP routers that are peers that reside in two different autonomous systems.

**Extranet.** An extranet connects two or more intranets. If an intranet as a company’s internal Web site enables users inside the company to communicate and exchange information, an extranet connects that virtual space with another company’s intranet, thus enabling these two (or more) companies to share resources and communicate over the Internet in their own virtual space. This technology greatly enhances business to business communications.

**Filters.** A filter organizes log entries based on admin specifications.
Firewall. A firewall device that protects and controls incoming and outgoing traffic on network connections. Firewalls protect internal servers from damage (intentional or otherwise) and enable authorized external access.

Gateway. Also called a router, a gateway is a program or a special-purpose device that transfers IP datagrams from one network to another until the final destination is reached.

GBIC. A Gigabit Interface Connector (GBIC) is the kind of interface module card used on some security devices for connecting to a fiber optic network.

GGSN. Gateway GPRS Support Node.

Gi Interface. The interface between a GSN and an external network or the Internet.

Global Domain. A domain is a logical grouping of devices, their policies, and their access privileges. The global domain is the top level, or root domain, that contains all subdomains.

GMT (Greenwich Mean Time). GMT is the Greenwich, England mean solar time. GMT is also known as Universal Time and is used for calculating time worldwide.

Gn Interface. The interface between two GSNs within the same PLMN.

Gp Interface. The interface between two GSNs located in different PLMNs.

G-PDU. A G-PDU is a user data message. It consists of a T-PDU plus a GTP header.

GPRS. General Packet Radio Service. A packet-based technology that enables high-speed wireless Internet and other data communications. GPRS provides more than three to four times greater speed than conventional GSM systems. Using a packet data service, subscribers are always connected and always online so services are easy and quick to access.

Group Expression Objects. A Group Expression Object represents a statement that sets conditions for authentication requirements, enabling you to combine multiple external user objects. You can create group expressions using the operator OR, AND, or NOT to combine user objects, user group objects, or other group expressions.

Groups. A group organizes previously-created devices into user-defined groups that make it easier for you to configure and manage devices in your domain. Groups enable you to execute certain NetScreen-Security Manager operations on multiple security devices at the same time.

GRX. GPRS Roaming Exchange.

GSM. Global System for Mobile Communications.

GTP Tunnel. A GTP tunnel in the GTP-U plane is defined for each PDP Context in the GSNs. A GTP tunnel in the GTP-C plane is defined for all PDP Contexts with the same PDP address and APN (for Tunnel Management messages) or for each MS (for messages not related to Tunnel Management). A GTP tunnel is identified in each node with a TEID, an IP address and a UDP port number. A GTP tunnel is necessary to forward packets between an external network and an MS user.

GTP. GPRS Tunneling Protocol.

GTP-C Message. GTP-Control Message. Control plane messages are exchanged between GSN pairs in a path. The control plane messages are used to transfer GSN capability information between GSN pairs, to create, update and delete GTP tunnels and for path management.

GTP-PDU. A GTP Protocol Data Unit is either a GTP-C message or a GTP-U message.
**GTP-U Message.** GTP-User Data message. User plane messages are exchanged between GSN pairs or GSN/RNC pairs in a path. The user plane messages are used to carry user data packets, and signalling messages for path management and error indication.

**GUI Server.** The GUI Server manages the system resources and data that drives NetScreen-Security Manager functionality. The GUI Server contains the NetScreen-Security Manager databases, and centralizes information for devices, their configurations, attack and server objects, and policies.

**H.323** application layer gateway (ALG) lets you to secure Voice-over-IP (VoIP) communication between terminal hosts, such as IP phones and multimedia devices. In such a telephony system, gatekeeper devices manage call registration, admission, and call status for VoIP calls. Gatekeepers can reside in the two different zones, or in the same zone.

**Hardened System.** A hardened system is a secure server with all appropriate security patches and bug fixes; these systems are designed to resist penetration.

**Hello Interval.** The amount of time that elapses between instances of Hello Packets.

**Hello Packet.** A Hello packet is a message sent out to the current network to announce the presence of the current routing instance to the network. Hello packets aid in the discovery of neighbors and in a router being able to connect to other devices on the network. When an OSPF interface is created, the interface sends Hello packets to the network to announce itself.

**Histogram.** A histogram is a vertical graph that represents different amounts by thin, color-coded bands or bars. These bars represent a frequency distribution; heights of the bars represent observed frequencies.

**HLR.** Home Location Register.

**Hold Time.** In OSPF, the maximum amount of time between instances of initiating Shortest Path First (SPF) computations. In BGP, the maximum amount of time that elapses between message transmissions between a BGP speaker and its neighbor.

**ICMP Flood.** An ICMP flood contains ICMP pings so numerous that they overload a system with echo requests, causing the system to expend all its resources responding until it can no longer process valid network traffic. If you set a threshold to invoke ICMP flood attack protection when exceeded, ICMP flood attacks are recorded as statistics.

**IE.** Information Element.

**IKE Proposal Objects.** An IKE proposal is a set of encryption keys and authentication algorithms that is used to negotiate a VPN connection. An IKE Proposal Object is a representation of an IKE proposal in the NetScreen-Security Manager UI.

**Import Rules.** When you have two or more virtual routers on a security device, you can configure import rules on one virtual router that define which routes are allowed to learned from another virtual router. If you do not configure any import rules for a virtual router, all routes that are exported to that virtual router are accepted. See also Export Rules.

**IMSI.** International Mobile Station Identity.

**Internet Control Message Protocol (ICMP).** ICMP is a network-layer protocol that does not carry user data, but does encapsulate its messages in IP datagrams. ICMP provides a query and response system (with error-reporting) used to determine if another system on the network can receive and send data. An ICMP echo request is also known as a ping.
**Internet Key Exchange (IKE).** IKE is a method for exchanging keys for encryption and authentication over an unsecured medium, such as the Internet.

**Internet Protocol (IP).** IP is an Internet standard protocol that defines a basic unit of data called a datagram. A datagram is used in a connectionless, best-effort, delivery system. The Internet protocol defines how information gets passed between systems across the Internet.

**IP Address.** Each node on a TCP/IP network usually has an IP address. The IP address has a network number portion and a host number portion:

- Class A, >32,768 nodes, address format: nnn.hhh.hhh.hhh
- Class B, 256-32,768 nodes, address format: nnn.nnn.hhh.hhh
- Class C, <256 nodes, address format: nnn.nnn.nnn.hhh

This address format is called decimal dot format. The "n" represents a digit of a network number and "h" represents a digit of a host number; for example, 128.1.2.30. If you are sending data outside of your network, such as to the Internet, you need to obtain the network number from a central authority, currently the Network Information Center. See also Subnet Mask.

**IP Gateway.** Also called a router, an IP gateway is a program or a special-purpose device that transfers IP datagrams from one network to another until the final destination is reached.

**IP Pool Objects.** An IP Pool object represents a range of IP addresses. Use IP Pool object to configure a DHCP server for your managed devices.

**IP Security (IPSec).** IPSec is a security standard maintained by the Internet Engineering Task Force (IETF). The IPSec protocol suite provides everything you need for secure communications—authentication, integrity, and confidentiality—and makes key exchange practical even in larger networks. See also DES-CBC, ESP/AH.

**IP Sweep.** An IP sweep is similar to a port scan attack. Attackers perform IP sweeps by sending ICMP echo requests (or pings) to different destination addresses and wait for replies that indicate the IP address of a target. If a remote host pings 10 addresses in 0.3 seconds, the security device flags the event as an IP sweep attack and drops the connection to prevent replies.

**IP Tracking.** A mechanism for monitoring configured IP addresses to see if they respond to ping or ARP requests. You can configure IP tracking with NSRP to determine device or VSD group failover. You can also configure IP tracking on a device interface to determine if the interface is up or down.

**ISAKMP.** The Internet Security Association and Key Management Protocol (ISAKMP) provides a framework for Internet key management and provides the specific protocol support for negotiation of security attributes. By itself, it does not establish session keys, however it can be used with various session key establishment protocols to provide a complete solution to Internet key management.

**Job Manager.** The Job Manager is a module of the NetScreen-Security Manager User Interface. Job Manager tracks the progress of the command as it travels to the device and back to the management server.

**Keepalive.** The amount of time in seconds that elapses between keepalive packets which ensures that the TCP connection between the local BGP router and a neighbor router is up. This value is equal to one-third of the hold time. The default is 60 seconds.
**Key Management.** The only reasonable way to protect the integrity and privacy of information is to rely upon the use of secret information in the form of private keys for signing and/or encryption. The management and handling of these pieces of secret information is generally referred to as “key management.” This includes the activities of selection, exchange, storage, certification, expiration, revocation, changing, and transmission of keys. Most of the work in managing information security systems lies in the key management.

**Land Attack.** During a Land Attack, attackers may send spoofed SYN packets that contain the IP address of the target as both the destination and source IP address to create an empty connection. These connections flood the target system, overwhelming it and causing a denial-of-service. You can configure security devices to block Land Attack and record Land Attack attempts.

**Link State Advertisement (LSA).** Link State Advertisements (LSAs) are the conveyance that enables OSPF routers to make device, network, and routing information available for the link state database. Each router retrieves information from the LSAs sent by other routers on the network to construct a picture of the entire internetwork from which they distill path information to use in the routing table.

**Link State.** Link state routing protocols operate using an algorithm commonly called the Shortest Path First (SPF) algorithm. Instead of relying on rumored information from directly connected neighbors as in distance vector protocols, each router in a link state system maintains a complete topology of the network and computes SPF information based on the topology.

**Load Balancing.** Load balancing distributes workload to processors to improve the throughput of a concurrent connections.

**Local Preference.** To provide better information than the Multi-Exit Discriminator (MED) value provides for a packet’s path selection, BGP provides an attribute known as the LOCAL_PREF or local preference value. You can configure the LOCAL_PREF attribute so that it has a higher value for prefixes received from a router that provides a desired path to be higher than prefixes heard on the router that provides a less desirable path. The higher the value, the more preferred the route. The LOCAL_PREF attribute is the metric most often used in practice to express preferences for one set of paths over another.

**Lockout.** Lockout is an object state during which the object cannot be edited.

**Log Category.** A log category defines the log type (alarm, config, traffic, and so on.).

**Log ID.** A log ID is a unique ID for the log entry, derived from the combination of the date and log number.

**Log Investigator.** The Log Investigator is a module of the NetScreen-Security Manager User Interface. The Log Investigator contains tools for analyzing your log entries in depth. Use the Log Investigator to manipulate and change constraints on log information, correlate log entries visually and rapidly, and filter log entries while maintaining the broader picture.

**Log Viewer.** The Log Viewer is a module of the NetScreen-Security Manager User Interface. The Log Viewer displays log entries that your security devices generate based on criteria that you defined in your Security Policies, on the Device Server, and in the device configuration. Logs appear in table format; each row contains a single log, and each column defines specific information for a log.

**Log.** A Log is a grouping of log entries.

**Loopback Interface.** A logical interface that emulates a physical interface on the security device, but is always in the up state as long as the device is up. You must assign an IP address to a loopback interface and bind it to a security zone.

**Main Display Area.** The main display area displays the content for the currently selected module or module contents.
Management System. The management system includes the GUI Server and Device Server. You can deploy the GUI Server and Device Server on separate servers; however, the combination of the two servers is known as the management system.

Mapped IP Address. A MIP is a direct one-to-one mapping of traffic destined for one IP address to another IP address.

MCC. Mobile Country Code.

MD5. Message Digest (version) 5 is an algorithm that produces a 128-bit message digest (or hash) from a message of arbitrary length. The resulting hash is used to verify authenticity.

Media Gateway Control Protocol (MGCP). MGCP is a text-based, application layer protocol that can be used for call setup and call control. The protocol is based on a master/slave call control architecture: the media gateway controller (call agent) maintains call control intelligence, and media gateways carry out the instructions from the call agent.

Member AS. The name of the autonomous system being included in a BGP confederation.

Menu Bar. The menu bar is the upper section of the NetScreen-Security Manager UI. The menu bar contains accessible commands.

Metric. A value associated with a route that the virtual router uses to select the active route when there are multiple routes to the same destination network with the same preference value. The metric value for connected routes is always 0. The default metric value for static routes is 1, but you can specify a different value when defining a static route.

MNC. Mobile Network Code.

Modeling. Modeling is the process of creating a non-deployed device configuration in the NetScreen-Security Manager UI.

Modules. A module is a first-level element in the NetScreen-Security Manager navigation tree.

MS. Mobile Station.

MSIN. Mobile Subscriber Identification Number.

NAT Object. A NAT Object is a global object that contains references to device-specific NAT configurations, enabling multiple devices to share a single object. Use the Device Manager to configure NAT for each device, then create a global NAT object that includes the device-specific NAT configuration. Use global NAT objects in Security Policies and VPNs; when you update a device, that device automatically replaces the global NAT object with its device-specific NAT configuration.

NAT-Traversal (NAT-T). A method for allowing IPSec traffic to pass through NAT devices along the data path of a VPN by adding a layer of UDP encapsulation. The method first provides a means for detecting NAT devices during Phase 1 IKE exchanges, and then a means for traversing them after Phase 2 IKE negotiations are complete.

Navigation Tree. The navigation tree displays the 11 NetScreen-Security Manager modules in the left pane of the NetScreen-Security Manager window.

Neighbor. To begin configuring a BGP network, you need to establish a connection between the current device and a counterpart, adjacent device known as a neighbor or peer. While this counterpart device may seem like unneeded information at first, it is actually central to the way BGP works. Unlike RIP or OSPF, you now have to configure two devices, both the current router and its neighbor, for BGP to work. While this requires more effort, it enables networking to occur on a larger scale as BGP eludes deploying the limited advertising techniques inherent to interior networking standards.
NetScreen Redundancy Protocol (NSRP). NRSP is a proprietary protocol that provides configuration and run time object (RTO) redundancy and a device failover mechanism for security devices in a high availability (HA) cluster.

NetScreen-Security Manager admin(istrator). The NetScreen-Security Manager admin is the person who uses NetScreen-Security Manager User Interface to manage their security devices.

Network Address Translation (NAT). NAT is a standard for translating secure IP addresses to temporary, external, registered IP address from the address pool. NAT enables trusted networks with privately assigned IP addresses to access the Internet, eliminating the need to use a registered IP address for every machine in your network.

NSAPI. Network Service Access Point Identifier.

NSGP. NetScreen Gatekeeper Protocol.

Object Manager. The Object Manager is a module of the NetScreen-Security Manager User Interface. The Object Manager contains the Objects used in your NetScreen-Security Manager system. An object is a re-usable, basic NetScreen-Security Manager building block that contains specific information; you use objects to create device configurations, policies, and VPNs. All objects are shared, meaning that they can be shared by all devices and policies in the domain.

Object. Objects represent reusable information, such as network addresses, individual users and user groups, and commonly used configuration data. In NetScreen-Security Manager, objects are shared objects, meaning they are shared between the global domain and all subdomains. Objects are the building blocks of the NetScreen-Security Manager management system.

On-Site Admin. The on-site admin is the person who installs a configlet using Rapid Deployment.

Open Shortest Path First (OSPF). A dynamic routing protocol intended to operate within a single Autonomous System.

Packet Filtering. Packet filtering is a router/firewall process that uses access control lists (ACL) to restrict flow of information based on protocol characteristics such as source/destination IP address, protocol, or port used. Generally, packet-filtering routers do not track sessions except when doing NAT (which tracks the session for NAT purposes).

PDP Context. A user session on a GPRS network.

PDP. Packet Data Protocol.

PDU. Protocol Data Unit.

Peer. See Neighbor

Ping of Death. The ping of death is an intentionally oversized or irregular ICMP packet that can trigger a Denial of Service condition, freezing, or other adverse system reactions. You can configure a security device to detect and reject oversized or irregular packet sizes.

PLMN. Public Land Mobile Network. A public network dedicated to the operation of mobile radio communications.

Point-to-Multipoint Network. A non-broadcast network where OSPF treats connections between routers as point-to-point links. There is no election of a designated router and no LSA generated for the network. A router in a point-to-multipoint network sends Hello packets to all neighbors with which it can directly communicate.
**Point-to-Point Network.** Joins two routers over a Wide Area Network (WAN). An example of a point-to-point network is two security devices connected via an IPSec VPN tunnel. On point-to-point networks, the OSPF router dynamically detects neighbor routers by sending Hello packets to the multicast address 224.0.0.5.

**Point-to-Point Protocol over Ethernet (PPPoE).** Allows multiple users at a site to share the same digital subscriber line, cable modem, or wireless connection to the Internet. You can configure PPPoE client instances, including the user name and password, on any or all interfaces on some security devices.

**Policy.** A Security Policy is the combination of both firewall rulebases and all rules into a comprehensive plan that defines how the security device works on your network.

**Port Address Translation (PAT).** The translation of the original source port number in a packet to a different, randomly designated port number.

**Port Mapping.** The translation of the original destination port number in a packet to a different, predetermined port number.

**Port Mode.** A feature supported on some security devices, port mode allows you to select one of several different sets of port, interface, and zone bindings on the device. Changing the port mode removes any existing configurations on the device and requires a system reset.

**Port Scan.** A port scan attack occurs when packets are sent out to different port numbers, for the purpose of scanning the available services in hopes that one port will respond. If a remote host scans 10 ports in 0.3 seconds, the security device flags this as a port scan attack and drops the connection.

**Preference.** A value associated with a route that the virtual router uses to select the active route when there are multiple routes to the same destination network. The preference value is determined by the protocol or origin of the route. The lower the preference value of a route, the more likely the route is to be selected as the active route.

**Prefix.** An IP address that represents a route.

**Process Status.** The process status displays information about processes on a security device.

**Protocol.** Protocols are predefined services (HTTP, SNMP, Telnet, and so on) that are enabled for the security device.

**PT.** Protocol Type.

**RADIUS.** Remote Authentication Dial-In User Service is a service for authenticating and authorizing remote access service (RAS) users.

**RAS (remote access services).** RAS is the acronym for remote access services, which enable users to access services protected by your security devices. Typically, you use a VPN to enable RAS, then add RAS users to the VPN.

**Real Time Streaming Protocol (RTSP).** RTSP is an application layer protocol for controlling the delivery of a stream of real-time multimedia content.

**Realtime Monitor.** The Realtime Monitor is a module of NetScreen-Security Manager User Interface. It contains the Device Monitor, the VPN Monitor, and the NSRP Monitor.

**Receive Collisions.** The number of collisions on the line detected by the Carrier Sense Multiple Access Collision Detection (CSMA/CD) protocol.

**Redistribution List.** A list of routes the current routing domain imported from another routing domain using a different protocol.
Redistribution. The process of importing a route into the current routing domain from another part of the network that uses another routing protocol. When this occurs, the current domain has to translate all the information, particularly known routes, from the other protocol. For example, if you are on an OSPF network and it connects to a BGP network, the OSPF domain has to import all the routes from the BGP network to inform all of its devices about how to reach all the devices on the BGP network. The receipt of all the route information is known as route redistribution.

Remote Procedure Call (RPC). The RPC is a protocol that one program can use to request a service from a program located in another computer in a network.

Remote Setting Objects. A Remote Settings object defines the DNS and WINS servers that are assigned to L2TP RAS users after they have connected to the L2TP tunnel.

Report Manager. Report Manager is a module of the NetScreen-Security Manager User Interface. Use Report Manager to generate and view reports summarizing log and alarm originating from the managed security devices in your network. You can use these reports to track and analyze log incidents, network traffic and potential attacks.

Role-Based Administration (RBA). Role-based administration enables you to define strategic roles for your administrators and create domains to organize your network devices. Use role-based administration to create a security environment that reflects your current offline administrator roles and responsibilities.

Route Flap Damping. BGP provides a technique to block the advertisement of the route somewhere close to the source until the route becomes stable. This method is called flap damping. Route flap damping allows routing instability to be contained at an AS border router adjacent to the region where instability is occurring. The impact of limiting the unnecessary propagation is to maintain reasonable route change convergence time as a routing topology grows.

Route Map. Route maps are used with BGP to control and modify routing information and to define the conditions by which routes are redistributed between routing domains. A route map contains a list of route map entries, each containing a sequence number and a match and a set value. The route map entries are evaluated in the order of an incrementing sequence number. Once an entry returns a matched condition, no further route maps are evaluated. Once a match has been found, the route map carries out a permit or deny operation for the entry. If the route map entry is not a match, then the next entry is evaluated for matching criteria.

Route Redistribution. Route redistribution is the exporting of route rules from one virtual router to another.

Route Reflector. A router whose BGP configuration enables readvertising of routes between Interior BGP (IBGP) neighbors or neighbors within the same BGP AS. A route reflector client is a device that uses a route reflector to readvertise its routes to the entire AS. It also relies on that route reflector to learn about routes from the rest of the network.

Routing Information Protocol (RIP). A dynamic routing protocol used within moderate-sized autonomous systems.

Routing Table. A list in a virtual router's memory that contains a real-time view of all the connected and remote networks to which a router is currently routing packets.

Rule. A rule is a statement that defines a specific type of network traffic. When traffic passes through the security device, the device attempts to match that traffic against its list of rules. If a rule is matched, the device performs the action defined in the rule against the matching traffic.

Run Time Object (RTO). A code object created dynamically in memory during normal operation. Some examples of RTOs are session table entries, ARP cache entries, certificates, DHCP leases, and IPSec Phase 2 security associations (SAs).

Schedule Object. A schedule object defines a time interval that a firewall rule is in effect. You use a schedule object in your firewall rule to determine when a device enforces that rule.

Secure Copy (SCP). A method of transferring files between a remote client and a security device using the SSH protocol. The security device acts as an SCP server, accepting connections from SCP clients on remote hosts.

Secure Server Protocol (SSP). For communication between the UI, the GUI Server, and the Device Server, NetScreen-Security Manager uses SSP, a modified version of TCP that is more reliable than ordinary TCP, requires less CPU and memory resources from servers, and reduces the number of acknowledgement packets on the network. SSP uses AES encryption and SH1 authentication for all connections.

Secure Shell (SSH). A protocol that allows device administrators to remotely manage the device in a secure manner. You can run either an SSH version 1 or version 2 server on the security device.

Security Association. The security association combines the Security Parameters Index and a destination address. Required for both Authentication Header and Encapsulating Security Payload protocols. See also Security Parameters Index.

security device. A security device enables access to your network components and protects your network against malicious traffic. NetScreen-Security Manager can manage security devices running ScreenOS 5.x and ScreenOs 4.0.x (except 4.0.2). All devices from NetScreen-5XT to the NetScreen-5400 are supported, except the NetScreen-5, NetScreen-10, and NetScreen-1000. NetScreen-Security Manager also supports the NetScreen-5GT running ScreenOS 4.0-DIAL2. NetScreen-Security Manager can also manage vsys configurations, NSRP clusters, and extranet devices.

Security Parameters Index (SPI). The SPI is a hexadecimal value which uniquely identifies each tunnel. It also tells the security device which key to use to decrypt packets.

Security Policies. A Security Policy defines access to your network, including permitted services, users, and time periods. Use Security Policies to control the shape of your network traffic as it passes through the firewall, or log specific network events.

Security Zone. A security zone is a collection of one or more network segments requiring the regulation of inbound and outbound traffic via access policies.

Server Manager. The Server Manager is a module of the NetScreen-Security Manager User Interface. Server Manager contains server objects that represent your management system components. Use Server Manager to manage and monitor the individual server processes that comprise your NetScreen-Security Manager system.

Service Object. Service objects represent the IP traffic types for existing protocol standards. Security devices monitor and manage network traffic using these protocols. NetScreen-Security Manager includes predefined service objects for most standard services. You can also create custom service objects to represent services that are not included in the list of predefined service objects, or to represent a custom service running on your network.
**Session Description Protocol (SDP).** SDP session descriptions appear in many SIP messages and provide information that a system can use to join a multimedia session. SDP might include information such as IP addresses, port numbers, times, dates, and information about the media stream.

**Session Initiation Protocol (SIP).** SIP is an IETF (Internet Engineering Task Force)-standard protocol for initiating, modifying, and terminating multimedia sessions over the Internet. Such sessions might include conferencing, telephony, or multimedia, with features such as instant messaging and application-level mobility in network environments.

**SGSN.** Serving GPRS Support Node.

**SHA-1.** Secure Hash Algorithm-1, an algorithm that produces a 160-bit hash from a message of arbitrary length. (It is generally regarded as more secure than MD5 because of the larger hashes it produces.)

**Shared Objects.** A shared object is an object that can be shared across domains.

**Short Frame.** A short frame contains less than 64 bytes of data.

**Signalling Message.** Any GTP-PDU except the G-PDU. GTP signalling messages are exchanged between GSN pairs in a path. The signalling messages are used to transfer GSN capability information between GSN pairs and to create, update and delete GTP tunnels.

**Source Interface-Based Routing (SIBR).** SIBR allows the security device to forward traffic based on the source interface (the interface on which the data packet arrives on the security device).

**Source Route.** The source route is an option in the IP header. An attacker can use the source route option to enter a network with a false IP address and have data sent back to the attacker’s real address.

**Stateful Inspection.** A firewall process that checks the TCP header for information on the session’s state. The process checks whether it is initializing (SYN), ongoing (SYN/ACK), or terminating (FIN). A stateful inspection firewall tracks each session flowing through it, dropping packets from unknown sessions that appear to be part of an ongoing or illegal sessions. All security devices are stateful inspectors.

**Static Routing.** User-defined routes that cause packets moving between a source and a destination to take a specified path. Static routing algorithms are table mappings established by the network administrator prior to the beginning of routing. These mappings do not change unless the network administrator alters them. Algorithms that use static routes are simple to design and work well in environments where network traffic is relatively predictable and where network design is relatively simple.

**Status Bar.** The status bar is the lower section of the NetScreen-Security Manager UI. The status bar displays supplemental information.

**Subdomain.** A subdomain is a domains under the global domain.

**Subinterface.** A subinterface is a logical division of a physical interface that borrows the bandwidth it needs from the physical interface from which it stems. A subinterface is an abstraction that functions identically to an interface for a physically present port and is distinguished by 802.1Q VLAN tagging.
Subnet Mask. A subnet mask enables you to define subnetworks. For example, if you have a class B network, a subnet mask of 255.255.255.0 specifies that the first two portions of the decimal dot format are the network number, while the third portion is a subnet number. The fourth portion is the host number. If you do not want to have a subnet on a class B network, you would use a subnet mask of 255.255.0.0. A network can be subnetted into one or more physical networks which form a subset of the main network. The Subnet Mask is the part of the IP address which is used to represent a subnetwork within a network. Using Subnet Masks enables you to use network address space which is normally unavailable and ensures that network traffic does not get sent to the whole network unless intended. See also IP address.

Super Admin(istrator). The super administrator is the default administrator for all domains. The superadmin has immutable powers. You cannot change or delete permissions for the super administrator; you can, however, change the password for the super admin.

SYN Attack. A SYN attack occurs when SYN packets overwhelm a network by initiating so many connection attempts or information requests that the network can no longer process legitimate connection requests, resulting in a Denial of Service.

Syslog. A protocol that enables a device to send log messages to a host running the syslog daemon (syslog server). The syslog server then collects and stores these log messages locally.

Tear Drop Attack. A Tear Drop Attack occurs when the first and second parts of a fragmented packet overlap, the server attempting to reassemble the packet can crash. If the security device sees this discrepancy in a fragmented packet, it drops the packet.

TEID. Tunnel Endpoint Identifier. The TEID uniquely identifies a tunnel endpoint in the receiving GTP-U or GTP-C protocol entity. The receiving end side of a GTP tunnel locally assigns the TEID value the transmitting side has to use. The TEID values are exchanged between tunnel endpoints using GTP-C messages.

Templates. A template is a device configuration that you can define once and then use for multiple devices. You can specify most device configuration values in a template. In a template, you can define only those configuration parameters that you want to set; you do not need to specify a complete device configuration.

The software remembers static routes until you remove them. However, you can override static routes with dynamic routing information through judicious assignment of administrative distance values. To do this, you must ensure that the administrative distance of the static route is higher than that of the dynamic protocol.

There are two types of BGP neighbors. internal neighbors which are in the same autonomous system and external neighbors which are in different autonomous systems. A reliable connection is required between neighbors and is achieved by creating a TCP connection between the two. The handshake that occurs between the two prospect neighbors evolves through a series of phases or states before a true connection can be made. See Connection States.

TID. Tunnel Identifier.

Toolbar. The toolbar is the upper section of the NetScreen-Security Manager UI. The toolbar contains icons that relate to accessible commands.

T-PDU. A T-PDU is the payload that is tunnelled in the GTP tunnel.

Transmission Control Protocol/Internet Protocol (TCP/IP). A set of communications protocols that support peer-to-peer connectivity functions for both local and wide area networks. A communications protocol which enables computers with different operating systems to communicate with each other. Controls how data is transferred between computers on the Internet.
Transmission Control Protocol/Internet Protocol (TCP/IP). TCP/IP is a set of communication protocols that support peer-to-peer connectivity functions for both local and wide area networks. (A communication protocol is a set of rules that allow computers with different operating systems to communicate with each other.) TCP/IP controls how data is transferred between computers on the Internet.

Triple DES (3DES). 3DES is a more powerful version of DES in which the original DES algorithm is applied in three rounds, using a 168-bit key. DES provides a significant performance savings but is considered unacceptable for many classified or sensitive material transfers.

Trojan. A trojan is a program with hidden functionality. Trojans often install a remote administration program (known as a backdoor) that enables attackers to access the target system.

Trunk Port. A trunk port enables a switch to bundle traffic from several VLANs through a single physical port, sorting the various packets by the VLAN identifier (VID) in their frame headers.

Trust Zone. One of two predefined zones that enables packets to be secured from being seen by devices external to your current domain.

Tunnel Interface. A tunnel interfaces is the opening, or doorway, through which traffic to or from a VPN tunnel passes. A tunnel interface can be numbered (that is, assigned an IP address) or unnumbered. A numbered tunnel interface can be in either a tunnel zone or security zone. An unnumbered tunnel interface can only be in a security zone that contains at least one security zone interface. The unnumbered tunnel interface borrows the IP address from the security zone interface.

Tunnel Zone. A tunnel zone is a logical segment that hosts one or more tunnel interfaces. A tunnel zone is associated with a security zone that acts as its carrier.

Tunneling. A method of data encapsulation. With VPN tunneling, a mobile professional dials into a local Internet Service Provider’s Point of Presence (POP) instead of dialing directly into their corporate network. This means that no matter where mobile professionals are located, they can dial a local Internet Service Provider that supports VPN tunneling technology and gain access to their corporate network, incurring only the cost of a local telephone call. When remote users dial into their corporate network using an Internet Service Provider that supports VPN tunneling, the remote user as well as the organization knows that it is a secure connection. All remote dial-in users are authenticated by an authenticating server at the Internet Service Provider’s site and then again by another authenticating server on the corporate network. This means that only authorized remote users can access their corporate network, and can access only the hosts that they are authorized to use.

UDP Flood. A UDP flood is an attack using multiple UDP packets. An attacker can send UDP packets to slow the target system to the point that it can no longer handle valid connections. You can configure the security device with a threshold to invoke UDP flood attack protection; when UDP packet flow exceeds this threshold, the device records the UDP flood attack as a statistics.

Universal Resource Locator (URL). A URL is a standard method of specifying the location of an available electronic resource. Also known as a location or address, a URL specifies the location of files on servers. A general URL has the syntax protocol://address. For example, http://www.srl.rmit.edu.au/pd/index.html specifies that the protocol is http and the address is www.srl.rmit.edu.au/pd/index.html.

Universal Unique Identifier (UUID). The UUID is a 128-bit number assigned to any object within a Distributed Computing Environment (DCE) cell which is guaranteed to be unique.

Untrust Zone. One of two predefined zones that enables packets to be seen by devices external to your current domain.
User Datagram Protocol (UDP). UDP is a protocol in the TCP/IP protocol suite that enables an application program to send datagrams to other application programs on a remote machine. UDP provides an unreliable and connectionless datagram service and does not guarantee delivery or duplicate detection; it does not use acknowledgments, or control the order of arrival.

User Interface (UI). The NetScreen-Security Manager graphical User Interface (UI) is used to control the NetScreen-Security Manager system. Using the UI, you can configure NetScreen-Security Manager administrators, add devices, edit policies, view reports, and so on.

User Object. User objects represent the users of your managed devices. You can include user objects or groups in Security Policies or VPNs to permit or deny access to individuals or groups.

User. A user is a person using the network your security devices are protecting. NetScreen-Security Manager supports two types of users: local users and external users.

View. A view is an admin-defined subset of column settings and filters in the Log Viewer.

Virtual IP Address. A VIP address maps traffic received at one IP address to another address based on the destination port number in the packet header.

Virtual Link. A logical path from a remote OSPF area to the backbone area.

Virtual Local Area Network (VLAN). A VLAN is a logical rather than physical grouping of devices that constitute a single broadcast domain. VLAN members are not identified by their location on a physical subnetwork but through the use of tags in the frame headers of their transmitted data. VLANs are described in the IEEE 802.1Q standard.

Virtual Private Network (VPN). A VPN is an easy, cost-effective and secure way for corporations to provide telecommuters and mobile professionals local dial-up access to their corporate network or to another Internet Service Provider (ISP). Secure private connections over the Internet are more cost-effective than dedicated private lines. VPNs are possible because of technologies and standards such as tunneling, screening, encryption, and IPSec.

Virtual Router (VR). A virtual router is the component of ScreenOS that performs routing functions. By default, a security device contains two virtual routers: Untrust-VR and Trust-VR.

Virtual security device (VSD). A VSD is a single logical device composed by a set of physical security devices.

Virtual Security Interface (VSI). A VSI is a logical entity at layer 3 that is linked to multiple layer 2 physical interfaces in a VSD group. The VSI binds to the physical interface of the device acting as master of the VSD group. The VSI shifts to the physical interface of another device in the VSD group if there is a failover and it becomes the new master.

Virtual System (VSYS). A virtual system is a subdivision of the main system that appears to the user to be a stand-alone entity. Virtual Systems reside separately from each other. Each one can be managed by its own Virtual System Administrator.

VPN Manager. VPN Manager is a module of the NetScreen-Security Manager User Interface. Use VPN Manager to design a system level VPN and automatically set up all connections, tunnels, and rules for all devices in the VPN.
**WebTrends.** A product offered by NetIQ that allows you to create customized reports based on the logs generated by a security device. When you use WebTrends, you can display the information you need in a graphical format.

**Windows Internet Naming Service (WINS).** WINS is a service for mapping IP addresses to NetBIOS computer names on Windows NT server-based networks. A WINS server maps a NetBIOS name used in a Windows network environment to an IP address used on an IP-based network.

**WinNuke Attack.** A WinNuke attack can crash any computer on the Internet running Windows by introducing a NetBIOS anomaly that forces Windows to restart. You can configure the security device to scan any incoming Microsoft NetBIOS Session Service packets, modify them, and record the event as a WinNuke attack.

**Worm.** A worm is a self-replicating attack program. Worms differ from typical viruses in that they are completely automatic—no attacker interaction is required. When the worm locates a vulnerable target, it immediately and automatically infects the new host with its malicious code. The newly infected host repeats the process and attempts to infect more hosts.

**XAuth.** A protocol composed of two components. remote VPN user authentication (user name plus password) and TCP/IP address assignments (IP address, netmask, DNS server, and WINS server assignments).

**Zone.** A zone can be a segment of network space to which security measures are applied (a security zone), a logical segment to which a VPN tunnel interface is bound (a tunnel zone), or either a physical or logical entity that performs a specific function (a function zone).
Appendix B

Unmanaged Commands

Juniper Networks NetScreen-Security Manager is designed for system-level management, enabling multiple administrators to manage their devices from one central location using the majority of CLI commands available in ScreenOS. However, a small number of device commands are unmanaged from the Juniper Networks NetScreen-Security Manager UI.

Most unmanaged commands are useful only when performing device administration on a specific device, and do not affect management capabilities (although future versions of NetScreen-Security Manager may support these commands). To use an unmanaged device command, you must connect locally to the Juniper Networks security device.

The table below details each unmanaged command.

Table 79: Unmanaged Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>common-criteria</td>
<td>This command disable all internal commands. Only the root admin can set this command. If someone other than the root admin tries to set this command, the security device displays an error message.</td>
</tr>
<tr>
<td>envar</td>
<td>These commands define environment variables. Security devices use environment variables to make special configurations at startup.</td>
</tr>
<tr>
<td>gate</td>
<td>This command checks the number of gates on a security device, how many are in use, and how many are still available. Gates are logical access points in the firewall for FTP and similar applications. Security devices create the gates, then convert a gate for each new session when data traffic occurs.</td>
</tr>
<tr>
<td>ike</td>
<td>These commands define the Phase 1 and Phase 2 proposals and the gateway for an AutoKey IKE (Internet Key Exchange) VPN tunnel, and specify other IKE parameters.</td>
</tr>
<tr>
<td>inter-vlan-traffic</td>
<td>These commands configure inter-VLAN traffic through a security device. It is possible to configure a virtual system (vsys) with two trusted interfaces, such that traffic can enter the vsys through one interface and exit through the other without undergoing any security services such as authentication or encryption. This is known as inter-VLAN traffic.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>set interface &lt;name&gt; dhcp client settings lease &lt;minute&gt;</td>
<td>This command configures settings affecting dhcp client lease time.</td>
</tr>
<tr>
<td>set log audit-loss-mitigation</td>
<td>This command configures logging to mitigate message loss due to memory limitations on a security device. Used for common criteria only.</td>
</tr>
<tr>
<td>set mac</td>
<td>This command configures a static Media Access Control (MAC) address for a security device interface.</td>
</tr>
<tr>
<td>timer</td>
<td>These commands display timer settings, or configure a security device to automatically execute management or diagnosis at a specified time. All timer settings remain in the configuration script after the specified time has expired.</td>
</tr>
<tr>
<td>user</td>
<td>These commands create, remove, or display entries in the internal user authentication database.</td>
</tr>
<tr>
<td>vr nsrp-config-sync</td>
<td>This command unsets synchronization for a specific virtual router in an NSRP cluster.</td>
</tr>
</tbody>
</table>
Appendix C  

SurfControl URL Categories

SurfControl servers maintain a database of millions of sites organized into about 40 categories. This Appendix contains a list of the categories maintained by SurfControl and a description of the URLs in each category.

Table 80: SurfControl URL Categories

<table>
<thead>
<tr>
<th>Category</th>
<th>Description of URLs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adult/Sexually Explicit</td>
<td>- Adult products including sex toys, CD-ROMs, and videos</td>
</tr>
<tr>
<td></td>
<td>- Adult services including video conferencing, escort services, and strip clubs</td>
</tr>
<tr>
<td></td>
<td>- Erotic stories and textual descriptions of sexual acts</td>
</tr>
<tr>
<td></td>
<td>- Explicit cartoons and animation</td>
</tr>
<tr>
<td></td>
<td>- Online groups, including newsgroups and forums, that are sexually explicit in nature</td>
</tr>
<tr>
<td></td>
<td>- Sexually-oriented or erotic full or partial nudity</td>
</tr>
<tr>
<td></td>
<td>- Depictions or images of sexual acts, including animals or inanimate objects used in a sexual manner</td>
</tr>
<tr>
<td></td>
<td>- Sexually exploitative or sexually violent text or graphics</td>
</tr>
<tr>
<td></td>
<td>- Bondage, fetishes, genital piercing</td>
</tr>
<tr>
<td></td>
<td>- Nudist sites that feature nudity</td>
</tr>
<tr>
<td></td>
<td>- Erotic or fetish photography, which depicts nudity</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> We do not include sites regarding sexual health, breast cancer, or sexually transmitted diseases (except in graphic examples).</td>
</tr>
</tbody>
</table>

Advertisements   | - Banner Ad Servers                                                                 |

Arts and Entertainment | - Television, movies, music and video programming guides     |
<p>|                      | - Downloadable (non-streaming) movie, video or sound clips   |
|                      | - Discussion forums on television, movies, music and videos   |
|                      | - Online magazines and reviews on the entertainment industry  |
|                      | - Celebrity fan sites                                        |
|                      | - Horoscopes                                                 |
|                      | - Online greeting cards                                       |
|                      | - Jokes, comics, comic books, comedians or any site designed to be funny or satirical |
|                      | - Circus, theatre, variety magazines, and radio               |
|                      | - Broadcasting firms and technologies (satellite, cable)      |
|                      | - Book reviews and promotions, publishing houses, and poetry  |
|                      | - Museums, galleries, artist sites (included sculpture, photography) |</p>
<table>
<thead>
<tr>
<th>Category</th>
<th>Description of URLs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chat</td>
<td>Web-based chat</td>
</tr>
<tr>
<td>Computing and Internet</td>
<td>Reviews, information, buyer’s guides of computers, computer parts and accessories, and software&lt;br&gt;ComputersoftwareInternet companies, industry news and magazines&lt;br&gt;Personal storage or backup&lt;br&gt;Pay-to-Surf sites&lt;br&gt;Freeware, shareware, and software downloads&lt;br&gt;Clipart, fonts and animated gif pages&lt;br&gt;Downloadable mobile phone/ PDA games, themes, graphics, and ringtones&lt;br&gt;Online photo albums/ digital photo exchange</td>
</tr>
<tr>
<td>Criminal Skills</td>
<td>Advocating, instructing, or giving advice on performing illegal acts such as phone, service theft, evading law enforcement, lock-picking, fraud, and burglary techniques&lt;br&gt;Plagiarism/cheating, including the sale of research papers</td>
</tr>
<tr>
<td>Drugs, Alcohol and Tobacco</td>
<td>Recipes, instructions or kits for manufacturing or growing illicit substances, including alcohol, for purposes other than industrial usage&lt;br&gt;Glamorizing, encouraging, or instructing on the use of or masking the use of alcohol, tobacco, illegal drugs, or other substances that are illegal to minors&lt;br&gt;Alcohol and tobacco promotional Web sites&lt;br&gt;Information on &quot;legal highs&quot;: glue sniffing, misuse of prescription drugs or abuse of other legal substances&lt;br&gt;Distributing alcohol, illegal drugs, or tobacco free or for a charge&lt;br&gt;Displaying, selling, or detailing use of drug paraphernalia&lt;br&gt;NOTE: We do not include sites that discuss medicinal drug use, industrial hemp use, or public debate on the issue of legalizing certain drugs. Nor do we include sites sponsored by a public or private agency that provides educational information on drug use.</td>
</tr>
<tr>
<td>Education</td>
<td>Educational institutions, including pre-, elementary, secondary, and high schools; universities.&lt;br&gt;Educational sites: pre-, elementary, secondary, and high schools; universities.&lt;br&gt;Distance education and trade schools, including online courses.&lt;br&gt;Online teacher resources (lesson plans)</td>
</tr>
<tr>
<td>Finance and Investment</td>
<td>Stock quotes, stock tickers, and fund rates&lt;br&gt;Online stock or equity trading&lt;br&gt;Online banking and bill-pay services&lt;br&gt;Investing advice or contacts for trading securities&lt;br&gt;Money management/investment services or firm&lt;br&gt;General finances and companies that advise thereof&lt;br&gt;Accountancy, actuaries, banks, mortgages, and general insurance companies</td>
</tr>
<tr>
<td>Food and Drink</td>
<td>Recipes, cooking instruction and tips, food products, and wine advisors&lt;br&gt;Restaurants, cafes, eateries, pubs, and bars&lt;br&gt;Food/drink magazines, reviews</td>
</tr>
<tr>
<td>Gambling</td>
<td>Online gambling or lottery web sites that invite the use of real or virtual money&lt;br&gt;Information or advice for placing wagers, participating in lotteries, gambling, or running numbers&lt;br&gt;Virtual casinos and offshore gambling ventures&lt;br&gt;Virtual sports leagues and sports picks and betting pools&lt;br&gt;NOTE: CasinoHotelResort sites that do not feature online gambling or provide gaming tips are categorized under Travel.</td>
</tr>
<tr>
<td>Category</td>
<td>Description of URLs</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| **Games**                     | - Game playing or downloading; game hosting or contest hosting  
                                 - Tips and advice on games or obtaining cheat codes ("cheatz")  
                                 - Journals and magazines dedicated to game playing                                                                                                           |
| **Glamour and Intimate Apparel** | - Lingerie, negligee or swimwear modeling  
                                 - Model fan pages; fitness models/sports celebrities  
                                 - Fashion or glamour magazines online  
                                 - Beauty and cosmetics  
                                 - Modeling information and agencies                                                                                                                        |
| **Government and Politics**   | - Government services such as taxation, armed forces, customs bureaus, emergency services.  
                                 - Local government sites  
                                 - Political debate, canvassing, election information and results  
                                 - Local, national, and international political sites                                                                                                      |
| **Hacking**                   | - Promotion, instruction, or advice on the questionable or illegal use of equipment and/or software for purpose of hacking passwords, creating viruses, gaining access to other computers and/or computerized communication systems.  
                                 - Sites that carry malicious executables or viruses  
                                 - Sites that provide instruction or work-arounds for our filtering software  
                                 - Cracked software and information sites  
                                 - Pirated software and multimedia download sites  
                                 - Sites that provide or promote parasites, including Spyware, Adware and other unsolicited commercial software                                                                 |
| **Hate**                      | - Advocating or inciting degradation or attack of specified populations or institutions based on associations such as religion, race, nationality, gender, age, disability, or sexual orientation  
                                 - Promoting a political or social agenda that is supremacist in nature and exclusionary of others based on their race, religion, nationality, gender, age, disability, or sexual orientation  
                                 - Holocaust revisionist/denial sites  
                                 - Coercion or recruitment for membership in a gang* or cult**  
                                 - Militancy, extremist  
                                 - Flagrantly insensitive or offensive material  
                                 **NOTE:** We do not include news, historical, or press incidents that may include the above criteria (except in graphic examples).  
                                 **A gang is defined as: a group whose primary activities are the commission of felonious criminal acts, which has a common name or identifying sign or symbol, and whose members individually or collectively engage in criminal activity in the name of the group.**  
                                 **A cult is defined as: a group whose followers have been deceptively and manipulatively recruited and retained through undue influence such that followers' personalities and behavior are altered. Leadership is all-powerful, ideology is totalistic, and the will of the individual is subordinate to the group. Sets itself outside of society.**
<table>
<thead>
<tr>
<th>Category</th>
<th>Description of URLs</th>
</tr>
</thead>
</table>
| Health and Medicine          | ■ General health such as fitness and well-being  
■ Medical information about ailments, conditions, and drugs  
■ Medical reference  
■ Medical procedures, including elective and cosmetic surgery  
■ Alternative and complementary therapies  
■ Prescription medicines  
■ Hospital, medical insurance  
■ Dentistry, optometry, and other medical-related sites  
■ General psychiatry and mental well-being sites  
■ Promoting self-healing of physical and mental abuses, ailments, and addictions  
■ Psychology, self-help books, and organizations |
| Hobbies and Recreation       | ■ Recreational pastimes such as collecting, gardening, kit airplanes  
■ Outdoor recreational activities such as hiking, camping, rock climbing  
■ Tips or trends focused on a specific art, craft, or technique  
■ Online publications on a specific pastime or recreational activity  
■ Online clubs, associations or forums dedicated to a hobby  
■ Traditional (board, card) games and their enthusiasts  
■ Animal/ pet related sites, including breed-specific sites, training, shows and humane societies |
| Hosting Sites                | ■ Web sites that host business and individuals’ web pages (such as GeoCities, earthlink.net, AOL) |
| Job Search and Career        | ■ Employment agencies, contractors, job listings, career information  
Development                   | ■ Career searches, career-networking groups |
| Kid's Sites                  | ■ Child oriented sites and sites published by children |
| Lifestyle and Culture        | ■ Homelife and family-related topics, including parenting tips, gay/lesbian/bisexual (non-pornographic sites), weddings, births, and funerals  
■ Foreign cultures, socio-cultural information |
| Motor Vehicles               | ■ Car reviews, vehicle purchasing or sales tips, parts catalogs  
■ Auto trading, photos, discussion of vehicles including motorcycles, boats, cars, trucks and RVs  
■ Journals and magazines on vehicle modification, repair, and customizing  
■ Online automotive enthusiast clubs |
| News                         | ■ Newspapers online  
■ Headline news sites, newswire services, and personalized news services  
■ Weather sites |
| Personals and Dating         | ■ Singles listings, matchmaking and dating services  
■ Advice for dating or relationships; romance tips and suggestions |
| Photo Searches               | ■ Sites that provide resources for photo and image searches |
| Real Estate                  | ■ Home, apartment, and land listings  
■ Rental or relocation services  
■ Tips on buying or selling a home  
■ Real estate agents  
■ Home improvement and inspection sites |
## Appendix C: SurfControl URL Categories

<table>
<thead>
<tr>
<th>Category</th>
<th>Description of URLs</th>
</tr>
</thead>
</table>
| Reference     | ■ Personal, professional, or educational reference  
■ Online dictionaries, maps, and language translation sites  
■ Census, almanacs, and library catalogues  
■ Topic-specific search engines                                                                                  |
| Religion      | ■ Churches, synagogues, and other houses of worship  
■ Any faith or religious beliefs, including non-traditional religions such as Wicca and witchcraft                                                   |
| Remote Proxies| ■ Remote proxies or anonymous surfing  
■ Web-based translation sites that circumvent filtering  
■ Peer-to-peer sharing                                                                                           |
| Sex Education | ■ Pictures or text advocating the proper use of contraceptives  
■ Sites relating to discussion about the use of the Pill, IUDs and other types of contraceptives  
■ Discussion sites on how to talk to your partner about diseases, pregnancy and respecting boundaries       |

**NOTE:** Not included in the category are commercial sites that sell sexual paraphernalia. These sites are typically found in the Adult category.

<table>
<thead>
<tr>
<th>Search Engines</th>
<th>■ General search engines (Yahoo, AltaVista, Google)</th>
</tr>
</thead>
</table>
| Shopping      | ■ Online auctions  
■ Department stores, retail stores, company catalogs and other sites that allow online consumer shopping  
■ Online downloadable product warehouses; specialty items for sale  
■ Freebies or merchandise giveaways                                                                                              |
| Sports        | ■ Team or conference web sites  
■ National, international, college, professional scores and schedules  
■ Sports-related online magazines or newsletters                                                                                  |
| Streaming Media| ■ Streaming media files or events (any live or archived audio or video file)  
■ Internet TV and radio  
■ Personal (non-explicit) webcam sites  
■ Telephony sites that allow users to make calls via the Internet                                                                         |
| Travel        | ■ Airlines and flight booking agencies  
■ Accommodation information  
■ Travel package listings  
■ City guides and tourist information  
■ Weather bureaus  
■ Car Rentals                                                                                                                      |
| Usenet News/Forums | ■ Newsgroups  
■ Opinion or discussion forums  
■ Weblog (blog) sites                                                                                                             |
| Usenet News/Forums | ■ Newsgroups  
■ Opinion or discussion forums  
■ Weblog (blog) sites                                                                                                             |
<table>
<thead>
<tr>
<th>Category</th>
<th>Description of URLs</th>
</tr>
</thead>
</table>
| Violence/Offensive| - Portraying, describing or advocating physical assault against humans, animals, or institutions  
  - Depictions of torture, mutilation, gore, or horrific death  
  - Advocating, encouraging, or depicting self-endangerment, or suicide, including through eating disorders or addictions  
  - Instructions, recipes or kits for making bombs or other harmful or destructive devices  
  - Excessive use of profanity or obscene gesticulation  
  - Sites promoting terrorism  
  - Excessively violent sports or games  
  - Offensive or violent language or satire  
  **NOTE:** We do not block news, historical, or press incidents that may include the above criteria (except in graphic examples). |
| Weapons           | - Online purchasing or ordering information, including lists of prices and dealer locations  
  - Any page or site predominantly containing, or providing links to, content related to the sale of guns, weapons, ammunition or poisonous substances  
  - Displaying or detailing the use of guns, weapons, ammunition or poisonous substances  
  - Clubs which offer training on machine guns, automatics and other assault weapons and/or sniper training  
  **NOTE:** Weapons are defined as something (as a club, knife, or gun) used to injure, defeat, or destroy. |
| Web-based E-mail  | - Web-based e-mail accounts  
  - Messaging sites |
Appendix D
Log Entries

This appendix lists the log entry subcategories for the following log entry categories:

- Screen Alarm Log Entries
- Alarm Log Entries
- Deep Inspection Alarm Log Entries
- Configuration Log Entries
- Information Log Entries
- Self Log Entries
- Traffic Log Entries

Additionally, you can also view the information provided for Basic and Extended GTP Log Entries.
Screen Alarm Log Entries

The Screen category contains the following subcategories:

Table 81: Screen Alarm Log Entries

<table>
<thead>
<tr>
<th>Attack</th>
<th>ScreenOS Message ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address Sweep Attack</td>
<td>Attacks &gt; Alert &gt; 00017</td>
</tr>
<tr>
<td>Block ActiveX component</td>
<td>Attacks &gt; Critical &gt; 00434</td>
</tr>
<tr>
<td>Block EXE component</td>
<td>Attacks &gt; Critical &gt; 00433</td>
</tr>
<tr>
<td>Block IP fragment traffic</td>
<td>Attacks &gt; Critical &gt; 00429</td>
</tr>
<tr>
<td>Block JAVA component</td>
<td>Attacks &gt; Critical &gt; 00432</td>
</tr>
<tr>
<td>Block ZIP component</td>
<td>Attacks &gt; Critical &gt; 00431</td>
</tr>
<tr>
<td>Destination IP session limit</td>
<td>Attacks &gt; Critical &gt; 00430</td>
</tr>
<tr>
<td>ICMP Flood Attack</td>
<td>Attacks &gt; Alert &gt; 00011</td>
</tr>
<tr>
<td>IDS ICMP Fragment</td>
<td>Attacks &gt; Critical &gt; 00422</td>
</tr>
<tr>
<td>IDS ICMP too large</td>
<td>Attacks &gt; Critical &gt; 00436</td>
</tr>
<tr>
<td>IDS IP Bad Options</td>
<td>Attacks &gt; Critical &gt; 00415</td>
</tr>
<tr>
<td>IDS IP unknown port</td>
<td>Attacks &gt; Critical &gt; 00414</td>
</tr>
<tr>
<td>IDS SYN Fragment</td>
<td>Attacks &gt; Critical &gt; 00412</td>
</tr>
<tr>
<td>IDS TCP FIN No ACK</td>
<td>Attacks &gt; Critical &gt; 00438</td>
</tr>
<tr>
<td>IDS TCP SYN FIN</td>
<td>Attacks &gt; Critical &gt; 00437</td>
</tr>
<tr>
<td>IDS TCP No Flag</td>
<td>Attacks &gt; Critical &gt; 00413</td>
</tr>
<tr>
<td>IP Source Route Attack</td>
<td>Attacks &gt; Alert &gt; 00009</td>
</tr>
<tr>
<td>IP Spoof Attack</td>
<td>Attacks &gt; Alert &gt; 00008</td>
</tr>
<tr>
<td>Land Attack</td>
<td>Attacks &gt; Alert &gt; 00010</td>
</tr>
<tr>
<td>Malicious URL Protection</td>
<td>Attacks &gt; Critical &gt; 00032</td>
</tr>
<tr>
<td>Multiple Authentications Failed</td>
<td>Auth &gt; Alert &gt; 00003</td>
</tr>
<tr>
<td>Ping of Death Attack</td>
<td>Attacks &gt; Emergency &gt; 00007</td>
</tr>
<tr>
<td>Policy Denied</td>
<td>Policies &gt; Alert &gt; 00018</td>
</tr>
<tr>
<td>Port Scan Attack</td>
<td>Attacks &gt; Alert &gt; 00016</td>
</tr>
<tr>
<td>SYN Attack</td>
<td>Attacks &gt; Emergency &gt; 00005</td>
</tr>
<tr>
<td>SYN Flood</td>
<td></td>
</tr>
<tr>
<td>SYN ACK</td>
<td></td>
</tr>
<tr>
<td>SYN MAC</td>
<td></td>
</tr>
<tr>
<td>SYN-ACK-ACK proxy DoS</td>
<td>Attacks &gt; Critical &gt; 00439</td>
</tr>
<tr>
<td>Source IP session limit</td>
<td>Attacks &gt; Critical &gt; 00033</td>
</tr>
<tr>
<td>Tear Drop Attack</td>
<td>Attacks &gt; Emergency &gt; 00006</td>
</tr>
<tr>
<td>UDP Flood Attack</td>
<td>Attacks &gt; Alert &gt; 00012</td>
</tr>
<tr>
<td>VPN Replay Detected</td>
<td>IKE &gt; Critical &gt; 00042</td>
</tr>
<tr>
<td>Winnuken Attack</td>
<td>Attack &gt; Alert &gt; 00004</td>
</tr>
</tbody>
</table>
The Alarm category contains the following subcategories:

<table>
<thead>
<tr>
<th>Alarm Log Entry Subcategories</th>
<th>ScreenOS Message ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin</td>
<td>Admin &gt; Alert &gt; 00027</td>
</tr>
<tr>
<td>Anti Virus - CSP</td>
<td>AntiVirus Scanning (External) &gt; Error &gt; 52</td>
</tr>
<tr>
<td>BGP Alarm</td>
<td>BGP &gt; Alert &gt; 00206</td>
</tr>
<tr>
<td>CPU Usage High</td>
<td>Logging &gt; Critical &gt; 00030</td>
</tr>
</tbody>
</table>
| DHCP                          | DHCP > Alert > 00029  
|                               | DHCP > Critical > 00029 |
| DNS Host                      | DNS > Critical > 00021 |
| Interface Failover            | Interface > Critical > 00090 |
| Hardware                      | Device > Critical > 00022 |
| IP Conflict                   | ARP > Critical > 00031 |
| Log Overflow                  | Logging > Critical > 00024 |
| Memory Low                    | Device > Critical > 00020  
|                               | Logging > Critical > 00020 |
| NSRP Inconsistent Config      | High Availability > 00015 |
| NSRP IP DUP Master            | High Availability > 00015 |
| NSRP RTO DOWN                 | High Availability > 00015 |
| NSRP RTO Duplicate            | High Availability > 00015 |
| NSRP RTO UP                   | High Availability > 00015 |
| NSRP Status                   | High Availability > Critical > 00015 |
| NSRP TRACKIP Failed           | High Availability > 00062 |
| NSRP TRACKIP Failover         | High Availability > 00062 |
| NSRP VSD 2nd Path Reply       | High Availability > Critical > 00077 |
| NSRP VSD 2nd Path REQ         | High Availability > Critical > 00076 |
| NSRP VSD Backup               | High Availability > Critical > 00073 |
| NSRP VSD Ineligible           | High Availability > Critical > 00074 |
| NSRP VSD Init                 | High Availability > Critical > 00070 |
| NSRP VSD Inoperable           | High Availability > Critical > 00075 |
| NSRP VSD Master               | High Availability > Critical > 00071 |
| NSRP VSD Pbackup              | High Availability > Critical > 00072 |
| OSPF Packet Flood             | OSPF > Critical > 00206 |
| RIP Packet Flood              | RIP > Critical > 207 |
| Route add/delete Error        | OSPF > Critical > 200 |
| Route RIP Updated Flood       | RIP > Critical > 00207 |
| Exceeded Route Entry (Sys)    | Route > Critical > 00200 |
| Secure Shell                  | SSH > Critical > 00034 |
Deep Inspection Alarm Log Entries

The Deep Inspection Alarm category contains the following subcategories:

<table>
<thead>
<tr>
<th>Attack Name</th>
<th>Attack Description</th>
<th>Severity</th>
<th>Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>APP:CURL-OF-BANNER</td>
<td>This signature detects buffer overflow attempts against the cURL file retrieval client. cURL 6.1 to 7.4 versions are vulnerable. Attackers may use a malicious server to connect to the cURL client and execute arbitrary code with the permissions of the cURL user.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>CHAT:AIM:MESSAGE-SEND</td>
<td>This signature detects messages sent from AIM clients to other AIM clients.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>CHAT:AUDIT:AIM:INVALID-TLV</td>
<td>This protocol anomaly is a AIM message with an invalid TLV; the TLV data specified in the FLAP header is less than the actual data in the TLV header.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>CHAT:AUDIT:AIM:INV-TLV-LEN</td>
<td>This protocol anomaly is a AIM message with an invalid TLV; the TLV length is less than expected, or the TLV length is greater than the data specified in the FLAP header.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>CHAT:AUDIT:MSN:GROUP-NAME</td>
<td>This protocol anomaly is an MSN message with a group name length that exceeds the user-defined maximum. The default group name maximum is 64.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>CHAT:AUDIT:YMSG:FILE-SEND</td>
<td>This signature detects a Yahoo Messenger client sending a file to another user.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>CHAT:AUDIT:YMSG:MAIL-ADDR</td>
<td>This protocol anomaly is a Yahoo! Messenger email address that exceeds the user-defined maximum. A Yahoo! Messenger server sends an email address as part of a new email alert message. The default number of bytes in an Yahoo! Messenger email address is 84.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>CHAT:AUDIT:YMSG:MSG-TOO-BIG</td>
<td>This protocol anomaly is a Yahoo! Messenger message that exceeds the user-defined maximum. The default number of bytes in an Yahoo! Messenger message is 8192.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>CHAT:AUDIT:YMSG:OFLOW-GRP-NAME</td>
<td>This protocol anomaly is a Yahoo! Messenger group name that exceeds the user-defined maximum. Yahoo! Messenger clients use groups to separate their friends into categories. The default number of bytes in an Yahoo! Messenger group name is 84.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>CHAT:AUDIT:YMSG:OFLOW-PASSWD</td>
<td>This protocol anomaly is a Yahoo! Messenger encrypted password that exceeds the user-defined maximum. The Yahoo! Messenger client sends an encrypted password to the server as part of the authentication process. The default number of bytes in an Yahoo! Messenger encrypted password is 1024.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>CHAT:MSN:ACCESS</td>
<td>This signature detects MSN Messenger chat using the specified content type &quot;text/plain&quot; on port 1863 (default port of MSN Messenger).</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>CHAT:MSN:LOGIN-ATTEMPT</td>
<td>This signature detects attempts to login to the MSN network using an MSN Messenger client.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>DB:MS-SQL:SQLXML-ISAPI-OF</td>
<td>This signature detects buffer overflow attempts against the SQLXML-ASAPI Extension in Microsoft SQL Server 2000. The SQLXML-ASAPI extension handles data queries over HTTP (SQLXML HTTP); attackers may connect to the target host and submit maliciously crafted data to create a buffer overflow.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>DNS:AUDIT:CLASS-NON-IN</td>
<td>This protocol anomaly is a DNS request/reply in which the question/resource address class is not IN (Internet Address). Although allowed by the RFC, this should happen only in rare circumstances and may indicate an exploit attempt.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>DNS:AUDIT:QCLASS-UNEXP</td>
<td>This protocol anomaly is a DNS reply with a resource specifying a CLASS ID reserved for queries only (QCLASS). This may indicate an exploit attempt.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>DNS:AUDIT:REP-QTYPE-UNEXPECTED</td>
<td>This protocol anomaly is a DNS reply with a resource specifying a TYPE ID reserved for queries only (QTYPE). This may indicate an exploit attempt.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>DNS:AUDIT:REP-S2C-QUERY</td>
<td>This protocol anomaly is a DNS reply with a query/reply bit (QR) that is unset (indicating a query). This may indicate an exploit attempt.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>DNS:AUDIT:REQ-C2S-RESPONSE</td>
<td>This protocol anomaly is a DNS request with a query/reply bit (QR) set (indicating a reply). This may indicate an exploit attempt.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>DNS:AUDIT:REQ-INVALID-HDR-RA</td>
<td>This protocol anomaly is a client-to-server DNS message with the recursion-available bit (RA) set. This may indicate an exploit attempt.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>DNS:AUDIT:TYPE-ALL</td>
<td>This protocol anomaly is a DNS request with request type set to &quot;ALL&quot;.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>DNS:EXPLOIT:EMPTY-UDP-MSG</td>
<td>This protocol anomaly is an empty DNS UDP message. This may indicate an exploit attempt.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>DNS:EXPLOIT:EXPLOIT-BIND9-RT</td>
<td>This protocol anomaly is an rdataset parameter to the dns_message_findtype() function in message.c that is not NULL. In BIND 9 (up to 9.2.0), attackers may cause a shutdown on an assertion failure. Note: Common queries in routine operations (such as SMTP queries) may trigger this anomaly.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>DNS:EXPLOIT:POINTER-LOOP</td>
<td>This protocol anomaly is a DNS message with a set of DNS pointers that form a loop. This may indicate a denial-of-service (DoS) attempt.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>DNS:EXPLOIT:REQUEST-SHORT-MSG</td>
<td>This protocol anomaly is a DNS message that ended prematurely. This may indicate an exploit attempt.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>DNS:EXPLOIT:TYPE-AXFR</td>
<td>This protocol anomaly is a zone transfer attempt. This may indicate an attempt to obtain information about an entire domain.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>DNS:HEADERERROR:INVALID-OPCODE</td>
<td>This protocol anomaly is a DNS request/reply with an invalid value in the header OPCODE field. This may indicate an exploit attempt.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-------------</td>
<td>--------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>DNS:OVERFLOW:FF-FF-BIN</td>
<td>This signature detects attempts to create buffer overflows. Attackers may send maliciously crafted packets to DNS servers to overflow the buffer and gain root access.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>DNS:OVERFLOW:INVALID-LABEL-LEN</td>
<td>This protocol anomaly is a DNS request/reply with a label that exceeds the maximum length (63) specified in the RFC. This may indicate a buffer overflow attempt.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>DNS:OVERFLOW:INVALID-POINTER</td>
<td>This protocol anomaly is a DNS request/reply with a pointer that points beyond the end of the data. This may indicate a buffer overflow or denial-of-service (DoS) attempt.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>DNS:OVERFLOW:NAME-TOO-LONG</td>
<td>This protocol anomaly is a DNS name that exceeds 255 characters. This may cause problems for some DNS servers.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>DNS:OVERFLOW:NXT-OVERFLOW</td>
<td>This protocol anomaly is a suspiciously large NXT resource record in a DNS transaction. BIND versions 8.2 through 8.2.1 are vulnerable to a buffer overflow in the processing of NXT resource records.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>DNS:OVERFLOW:OPT-DOS</td>
<td>This protocol anomaly is a suspiciously long OPT resource record. All versions of BIND up to version 8.3.3 are vulnerable to a denial of service attack. An attacker can crash the server by requesting a subdomain that does not exist with an OPT resource record that has a very large UDP payload size.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>DNS:OVERFLOW:OVERSIZED-UDP-MSG</td>
<td>This protocol anomaly is a DNS UDP-based request/reply that exceeds the maximum length (512) specified in RFC. This may indicate a buffer overflow attempt.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>DNS:OVERFLOW:SIG-OVERFLOW</td>
<td>This protocol anomaly is a TCP-based DNS transaction with a suspiciously small SIG resource record. Bind versions 8 to 8.3.3 are vulnerable to a heap overflow in the code that handles SIG resource records. Attackers may execute arbitrary code on the server.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>DNS:OVERFLOW:TOO-LONG-TCP-MSG</td>
<td>This protocol anomaly is a DNS TCP-based request/reply that exceeds the maximum length specified in the message header. This may indicate a buffer overflow or an exploit attempt.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>DNS:QUERY:NULL-QUERY</td>
<td>This protocol anomaly is a DNS request with the question, answer, additional, and name server counts are zero. This can indicate a malicious user trying to crash the DNS server.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>DNS:QUERY:VERSION-QUERY</td>
<td>This protocol anomaly is a DNS query for version.bind with the type set to TXT and the class set to CHAOS. BIND servers support the ability to be remotely queried for their versions. This can indicate a reconnaissance attempt; when attackers know the BIND version, they can then attempt to exploit vulnerabilities on the server.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>DOS:NETDEV:CISCO-HTTPD-DOS</td>
<td>This signature detects attempts to exploit a vulnerability in Cisco IOS. Versions prior to 11.0, 11.2.8SA1, 12.1(1a)T1, and 12.1(1.3)T are susceptible. Attackers may remotely request URLs containing the %%% string from the IP HTTP server, causing the router to crash/reboot/power cycle.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>DOS:NETDEV:CISCO-RTR-DOS</td>
<td>This signature detects denial-of-service (DoS) attempts against Cisco (routers). Cisco has identified multiple affected versions of IOS and customers are advised to check with their vendor or on Cisco’s Web site for information. Attackers may send invalid HTTP traffic to a Cisco IOS device to cause a DoS on the device.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>--------------</td>
</tr>
<tr>
<td>DOS:NETDEV:LINKSYS-GOZILA-DOS2</td>
<td>This signature detects attempts to exploit a vulnerability in a LinkSys Cable/DSL router. Attackers may submit an overly long sysPasswd parameter within a malicious HTTP request to crash a LinkSys Cable/DSL router.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>DOS:NETDEV:LINKSYS-GOZILA-DOS3</td>
<td>This signature detects attempts to exploit a vulnerability in a LinkSys Cable/DSL router. Attackers may submit an overly long DomainName parameter within a malicious HTTP request to crash a LinkSys Cable/DSL router.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>DOS:NETDEV:NETWORK-3COM-DOS</td>
<td>This signature detects attempts to exploit a firmware vulnerability in the 3COM OfficeConnect 812 and 840 DSL/ADSL routers. OCR812 versions 1.1.9 and earlier are susceptible. Attackers may remotely request long strings from the HTTP daemon, making the router reboot/power cycle and creating a denial-of-service (DoS).</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>DOS:NETDEV:WEBJET-FRAMEWORK</td>
<td>This signature detects attempts to exploit a vulnerability in HP Web JetAdmin service. Web JetAdmin version 6.5 is vulnerable. Attackers may access sensitive configuration information. If you run an HP Web JetAdmin server on your network, configure DI to monitor the server port that is configured to listen; by default, the listening port is TCP/8000.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>DOS:NETDEV:WEBJET-FW-INFOLEAK</td>
<td>This signature detects attempts to exploit a vulnerability in HP Web JetAdmin service. Web JetAdmin version 6.5 is vulnerable. Attackers may access sensitive configuration information.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>DOS:NETDEV:WEBJET-TRAVERSAL</td>
<td>This signature detects directory traversal attempts against HP Web JetAdmin service. HP Web JetAdmin version 7.5.2546 and earlier are vulnerable. Because JetAdmin does not properly verify input to the setinclude parameter in /plugins/hpjdwm/script/test/setinfo.hts, attackers may use a directory traversal to read and execute arbitrary HTS files.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>DOS:NETDEV:WEBJET-WRITETOFILE</td>
<td>This signature detects attempts to exploit a vulnerability in HP Web JetAdmin service. Web JetAdmin versions 7.x are vulnerable. Attackers may send a maliciously formatted request to a Web JetAdmin script to execute arbitrary commands on the server.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>FTP:COMMAND:PLATFTP-CD-DOS</td>
<td>This signature detects attempts to exploit a vulnerability in PlatinumFTP. Attackers may submit a maliciously crafted pathname in a CD request to crash the FTP daemon. PlatinumFTP 1.0.6 and earlier versions are vulnerable.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:COMMAND:SITE-EXEC</td>
<td>This signature detects attempts to exploit a configuration vulnerability in wuFTPd. Version 2.4.1 is susceptible. pathnames.h sets _PATH_EXCEPATH to /bin, which is relative to ~ftp for anonymous users, but relative to / for users with accounts (specifying the actual /bin rather than ~ftp/bin). Attackers may establish an FTP account on the system and run the site exec command to gain access to the /bin directory.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:DIRECTORY:DOT-DOT</td>
<td>This signature detects ‘./..’ FTP commands sent to FTP/21. Attackers may change the directory to the root directory of the FTP service, and gain access to the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>FTP:DIRECTORY:MSIE-FTP-DIRTRA/</td>
<td>This signature detects a Microsoft Internet Explorer client attempting to download a file from a malicious server. The server may embed a directory traversal attack in the filename to specify the exact file download location on the client machine.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>FTP:EXPLOIT:BOUNCE-ATTACK</td>
<td>This protocol anomaly is an FTP bounce attack. There are two possibilities: a PORT command specified an IP address different from the client address, or a PASV command resulted in a 227 message with an IP address different than the server.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:EXPLOIT:FTPBIN-WRITEABLE</td>
<td>This signature detects an attempt by a malicious attacker to upload files with the names of common binaries to the FTP server's /bin directory. Successful exploitation of this vulnerability may result in the attacker being able to execute arbitrary code on the victim ftp server, including the reading of sensitive files outside of the ftp server's path.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>FTP:EXPLOIT:ILLEGAL-PORT</td>
<td>This protocol anomaly is an FTP PORT command/response to a PASV command (&quot;227...&quot;) that specifies a reserved port number. This may indicate an attempt to make the firewall open reserved ports.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:EXPLOIT:OPENFTPD-MSG-FS</td>
<td>This signature detects attempts to exploit a format string vulnerability in the OpenFTP daemon.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>FTP:EXPLOIT:SYNTAX-ERROR</td>
<td>This protocol anomaly is a syntax error in an FTP command/response, such as a malformed PORT command or 227 response. This may indicate an exploit attempt.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:EXPLOIT:TYPOFT-DOS</td>
<td>This signature detects denial-of-service (DoS) attempts against TypSoft FTP Server. TypSoft FTP Server 1.10 and earlier versions are vulnerable. Attackers may send known malicious FTP path strings to exhaust all system resources and crash a TypSoft FTP Server.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:EXPLOIT:WIN32-WFTPD-BOF</td>
<td>This signature detects invalid LIST, NLST, and STAT commands. WS-FTPD for Windows (trial versions 3.20 and 3.21, Pro and Standard) contains a vulnerability in the command parser that may allow malicious users to crash the service or execute arbitrary code.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>FTP:FILE:FTP-PUT-AUTOEXECBAT</td>
<td>This signature detects an attempt by an attacker to exploit a directory traversal vulnerability in the SunFTP daemon. Successful exploitation of this vulnerability may allow an attacker to read and write to files outside of the daemon's directory structure. This vulnerability is present in SunFTP build 9.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>FTP:MS-FTP:ASTERISK</td>
<td>This signature detects denial-of-service (DoS) attempts against Microsoft FTP Service in Microsoft IIS 4.0 and 5.0. Attackers who have previously established an FTP session may send glob characters within a maliciously crafted NLST request to crash the server.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:MS-FTP:STAT-GLOB</td>
<td>This signature detects denial-of-service (DoS) attempts against Microsoft FTP Service in Microsoft IIS 4.0 and 5.0. Attackers who have previously established an FTP session may send glob characters within a maliciously crafted status request to crash the server.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------------</td>
</tr>
<tr>
<td>FTP:OVERFLOW:BSD-FTPD-MKD-OF</td>
<td>This signature detects buffer overflow attempts against the FTPD that ships with early versions of FreeBSD 4.x and OpenBSD 2.8. FTPD 6.00LS and 6.5/OpenBSD versions are vulnerable. Attackers may gain local host access and root permissions.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:OVERFLOW:FREEBSD-FTPD-GLOB</td>
<td>This signature detects buffer overflow attempts against the FreeBSD FTP daemon. FreeBSD-4.2 is vulnerable. Attackers may submit a malicious STAT request that contains file globbing characters to execute arbitrary code on the target host with administrator privileges.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:OVERFLOW:LINE_TOO_LONG</td>
<td>This protocol anomaly is an incoming FTP line that is too long. This may indicate an attempt to overflow the server.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:OVERFLOW:OPENBSD-X86</td>
<td>This signature detects buffer overflow attempts against ftpd in OpenBSD. OpenBSD versions 2.7 and 2.8, FTP code revisions 1.49 to 1.79 are vulnerable. Attackers with write access may exploit the replydirname() function in BSD-based ftpd daemons to gain root access.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:OVERFLOW:PASS_TOO_LONG</td>
<td>This protocol anomaly is an FTP client password that exceeds the length threshold. This may indicate a malicious FTP client attempting to overflow the server.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:OVERFLOW:PATH-LINUX-X86-1</td>
<td>This signature detects attempts to exploit a realpath vulnerability in ProFTPD and wuFTPd running on LINUX. Versions ProFTPD 1.2pre1 and earlier and wuFTPd 2.4.2 (beta 18) VR9 and earlier are susceptible. Attackers may gain write access, remotely create long pathnames, and overflow the buffer to gain root access.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:OVERFLOW:PATH-LINUX-X86-2</td>
<td>This signature detects attempts to exploit a realpath vulnerability in ProFTPD and wuFTPd running on LINUX. Versions ProFTPD 1.2pre1 and earlier and wuFTPd 2.4.2 (beta 18) VR9 and earlier are susceptible. Attackers may gain write access, remotely create long pathnames, and overflow the buffer to gain root access.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:OVERFLOW:PATH-LINUX-X86-3</td>
<td>This signature detects attempts to exploit a realpath vulnerability in ProFTPD and wuFTPd running on LINUX. Versions ProFTPD 1.2pre1 and earlier and wuFTPd 2.4.2 (beta 18) VR9 and earlier are susceptible. Attackers may gain write access, remotely create long pathnames, and overflow the buffer to gain root access.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:OVERFLOW:PATH-TOO-LONG</td>
<td>This protocol anomaly is a pathname in an FTP command (RETR, STOR, APPE, SMNT, RNFR, RNTQ, DELE, RMD, MKD, STAT, CWD, LIST, NLST) that exceeds the length threshold. This may be an attempt to overflow the server.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:OVERFLOW:SITESTRING-2-LONG</td>
<td>This protocol anomaly is an argument in the FTP SITE command that exceeds the length threshold. This may be an attempt to overflow the server.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:OVERFLOW:USERNAME-2-LONG</td>
<td>This protocol anomaly is a username in an FTP connection that exceeds the length threshold. This may be an attempt to overflow the server.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:OVERFLOW:WFTPD-MKD-OVERFLOW</td>
<td>This signature detects buffer overflow attempts against the MKD command in Wftpd server 2.34. Attackers may use MKD and CWD commands to create nested directories and execute arbitrary commands with system privileges.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>------------</td>
</tr>
<tr>
<td>FTP:OVERFLOW:WUBSD-SE-RACE</td>
<td>This signature detects buffer overflow attempts against the PASS command in Wu-ftpd 2.6.0 and BSDI-ftpd. Attackers may send a maliciously crafted PASS request to an FTP server to execute arbitrary commands as root.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:PABLO-FTP:FORMAT-STRING</td>
<td>This signature detects denial-of-service attempts against the Pablo FTP Server. Versions 1.2, 1.3, and 1.5 running on Windows 2000 are vulnerable. Because the FTP server improperly parses format string characters, attackers may supply a maliciously crafted username to execute arbitrary code and crash the server.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:PASSWORD:BRUTE-FORCE</td>
<td>This protocol anomaly is multiple login failures within a short period of time between a unique pair of hosts.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>FTP:PASSWORD:COMMON-PASSWD</td>
<td>This signature detects common passwords used in FTP sessions. Attackers may attempt to log into known accounts using easily guessed passwords.</td>
<td>info</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:PASSWORD:H0TB0X</td>
<td>This signature detects attempts to use the default rootkit password 'h0tb0x' to access a FreeBSD rootkit account. Attackers may gain root access.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:PASSWORD:LRKR0X</td>
<td>This signature detects attempts to install the Rootkit hacker utility on a LINUX system. The default password is lrkr0x.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:PASSWORD:SATORI</td>
<td>This signature detects attempts to install the Rootkit lrk4 hacker utility on a system. The default password is satori.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:PASSWORD:WH00T</td>
<td>This signature detects attempts to install the Rootkit hacker utility on a LINUX system. The default password is wh00t.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:PROFTP:LOGKFR-OF1</td>
<td>This signature detects buffer overflow attempts against the log_xfer() function in ProFTPD. This vulnerability affects ProFTPD versions 1.2.0pre1, pre2, and pre3.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:PROFTP:MKD-OVERFLOW</td>
<td>This signature detects buffer overflow attempts against ProFTPD. Versions 1.2pre3 and earlier are vulnerable. Attackers may send a pathname to the ‘MKD’ command to gain remote root access.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:PROFTP:PPC-FS1</td>
<td>This signature detects attempts to exploit a format string vulnerability in ProFTPD. Versions 1.2pre6 and earlier are vulnerable. Attackers may overflow the PWD command.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:PROFTP:PPC-FS2</td>
<td>This signature detects attempts to exploit a format string vulnerability in ProFTPD. Versions 1.2pre6 and earlier are vulnerable.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:PROFTP:PROFTP-GEN-GLOB-DOS</td>
<td>This signature detects denial-of-service (DoS) attempts against ProFTPD. Because ProFTPD uses inadequate globbing algorithms, attackers may send wildcards in the argument of a maliciously crafted command to DoS the server.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:PROFTP:SIZE-DOS2</td>
<td>This signature detects attempts to exploit a vulnerability in ProFTPD. Version 1.2.0pre* is vulnerable. Attackers may send multiple SIZE requests with a static pathname to create a denial-of-service (DoS).</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:PROFTP:USER-DOS</td>
<td>This signature detects attempts to exploit a vulnerability in ProFTPD. Versions 1.2.0rc* and 1.2.0pre* are vulnerable. Attackers may send a maliciously crafted USER command to create a denial-of-service (DoS).</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-------------</td>
<td>--------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>FTP:REQERR:GNULS-WIDTH-DOS</td>
<td>This signature detects denial-of-service (DoS) attempts against GNU ls. If the FTP daemon uses a vulnerable version of GNU ls, attackers may send an oversized width parameter to GNU ls to cause the server CPU utilization to temporarily reach 100% and exhaust system memory. This condition can persist for several minutes depending on the width specified.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:REQERR:REQ-MISSING-ARGS</td>
<td>This protocol anomaly is an FTP command with an incomplete argument list, such as a USER command with no user name, a RETR command with no file name, etc. This may indicate command line access to the FTP server or an exploit attempt.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:SERVU:CHMOD-OVERFLOW</td>
<td>This signature detects attempts to exploit a vulnerability in the ServU FTP server CHMOD command. The CHMOD command is typically used to change the permissions of a file on the server. Attackers may send an overly long filename argument to the CHMOD command to execute arbitrary code with system privileges.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>FTP:USER:ROOT</td>
<td>This signature detects attempts to login to an FTP server using the “root” account. This may indicate an attacker trying to gain root-level access, or it may indicate poor security practices. FTP typically uses plain-text passwords, and using the root account to FTP could expose sensitive data over the network.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:WS-FTP:CPWD</td>
<td>This signature detects buffer overflow attempts against WS FTP Server. The code that handles arguments to the SITE CPWD command, which allows users to change their password, contains an unchecked string copy. Attackers may send a maliciously crafted argument in the SITE CPWD command to overflow the buffer and overwrite the return address.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:WU-FTP:DELE-OF</td>
<td>This signature detects buffer overflow attempts against the DELE command in a WU-ftpd server. Wu-ftpd versions 2.4 and prior (Academ beta12-18 included) are vulnerable. This may be a variation on the ADM exploit; attackers may log in anonymously using a hardcoded email address as the password.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:WU-FTP:FTPD-BSD-X86</td>
<td>This signature detects attempts to exploit an input validation vulnerability in wuFTpd running on FreeBSD. FreeBSD versions 4.3 and 4.4 are vulnerable. Because user input goes directly into a format string for a printf function, attackers may overwrite data on a stack (i.e. a return address), access the shellcode pointed to by the overwritten eip, and execute arbitrary commands.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:WU-FTP:GLOBARG</td>
<td>This signature detects attempts to exploit a vulnerability in Wu-ftpd, a software package that provides File Transfer Protocol (FTP) services for UNIX and Linux systems. Wu-ftpd versions 2.6.1 to 2.6.18 are vulnerable. Attackers may send a maliciously crafted pathname in a CWD or LIST command to the FTP server to execute arbitrary commands as root.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-------------</td>
<td>--------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>FTP:WU-FTP:IREPLY-FS</td>
<td>This signature detects attempts to exploit a format string vulnerability in Wu-ftpd 2.4 running on Solaris 2.8. Attackers may inject malicious code into the Wu-ftpd daemon memory space; later in the same session, the attacker may exploit a format string vulnerability in the Ireply() function to access that code and execute arbitrary commands as root.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:WU-FTP:LINUX-OF</td>
<td>This signature detects attempts to exploit an input validation vulnerability in wuFTPd running on LINUX. All versions are susceptible. Because user input goes directly into a format string for a *printf function, attackers may overwrite data on a stack, i.e. a return address, access the shellcode pointed to by the overwritten eip, and execute arbitrary commands. This same attack may be successful seen against ProFTPD servers.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:WU-FTP:REALPATH-OF</td>
<td>This signature detects buffer overflow attempts against the realpath() function in Wu-ftpd, a software package that provides File Transfer Protocol (FTP) services for UNIX and Linux systems. Wu-ftpd version 2.5.0 and earlier are vulnerable. Attackers may send a maliciously crafted FTP pathname to overflow a buffer in realpath() and execute arbitrary commands with administrator privileges.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:WU-FTP:REALPATH-OF2</td>
<td>This signature detects buffer overflow attempts against the realpath() function in Wu-ftpd, a software package that provides File Transfer Protocol (FTP) services for UNIX and Linux systems. Wu-ftpd version 2.5.0 and earlier are vulnerable. Attackers may send a maliciously crafted FTP pathname to overflow a buffer in realpath() and execute arbitrary commands with administrator privileges.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:3COM:3COM-PASS-LEAK</td>
<td>This signature detects attempts to access a 3COM wireless router web page that contains sensitive administrative information. No authentication is required to access this page.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:3COM:ADMIN-LOGOUT</td>
<td>This signature detects direct requests to the logout web service on a 3Com 3crwe754g72-a based device. Attackers that are spoofing a 3Com administrator’s IP address may call the logout application to force the administrator to logout.</td>
<td>info</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:3COM:CONF-DOWNLOAD</td>
<td>This signature detects attempts to download the configuration file from a 3Com 3crwe754g72-a based device. Attackers may use the sensitive information obtained from the configuration file to gain full control over the device.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:3COM:LOG-CLEAN</td>
<td>This signature detects attempts to cause a 3Com 3crwe754g72-a based device to clear its logs. Attackers may use spoofed IP address to send a log clear request without authenticating.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:APACHE:APACHE-BADIPV6</td>
<td>This signature detects attempts to exploit a vulnerability in Apache Web server. All Apache servers on all platforms running version Apache 2.0.50 and earlier are vulnerable. Using apr-util, attackers may include a crafted IPv6 literal address within an HTTP request to an Apache v2 server to cause the Apache child process to quit. On BSD systems, attackers may also be able to execute arbitrary code.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------------</td>
</tr>
<tr>
<td>HTTP:APACHE:APACHE-BADIPv6-2</td>
<td>This signature detects attempts to exploit a vulnerability in Apache Web server. All Apache servers on all platforms running version Apache 2.0.50 and earlier are vulnerable. Using apr-util, attackers may include a crafted IPv6 literal address within an HTTP request to an Apache v2 server to cause the Apache child process to quit. On BSD systems, attackers may also be able to execute arbitrary code.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:APACHE:CHUNKED-WORM</td>
<td>This signature detects attempts to infect Apache Web servers with the Apache Worm. Apache versions 1.3.26, 2.0.38 and prior are vulnerable. Apache improperly calculates required buffer sizes for chunked encoded requests due to a signed interpretation of an unsigned integer value. The worm sends POST requests containing malicious chunked encoded data to exploit the Apache daemon.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:APACHE:MOD-NTLM-BOF1</td>
<td>This signature detects buffer overflow attempts against Apache Web server. An Apache Web server uses mod_ntlm (an Apache 1.x and 2.x module) to authenticate users against a Microsoft Windows Domain Controller. Attackers may send long or malformed strings to mod_ntlm using the Authorization HTTP header, overflow the buffer, then execute arbitrary code on the Web server.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:APACHE:MODPHP-UPLOAD-HOF</td>
<td>This signature detects heap overflow attempts against mod_php in Apache. Attackers may send a maliciously crafted HTTP POST request to execute arbitrary code on the server.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:APACHE:NOSEJOB</td>
<td>This signature detects attempts to exploit a vulnerability in Apache Web servers. Apache improperly calculates required buffer sizes for chunked encoded requests due to a signed interpretation of an unsigned integer value. Attackers may send chunked encoded requests with the unique Host header value “Apache-nosejob.c.” in the GET request to create a buffer overflow and execute arbitrary code.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:APACHE:PHP-INVALID-HDR</td>
<td>This signature detects denial-of-service attempts against the Apache HTTP daemon. PHP versions 4.2.0 and 4.2.1 running on Apache 1.3.26 are vulnerable. Attackers may use invalid headers in an HTTP request to crash the Apache HTTP daemon; the daemon may require a manual restart.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:APACHE:REDHAT-DIRLIST</td>
<td>By submitting a malformed HTTP GET request to an Apache server using the default configuration supplied with several versions of RedHat Linux an attacker can cause the web server to return a listing of the contents of that directory, even if an index page is present.</td>
<td>low</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:APACHE:RESIN-WEB-INF</td>
<td>This signature detects attempts to exploit a flaw in Resin 2.1.12, a Java Scriptlet server. Attackers can send malformed URL requests to a server to allow access to a normally protected sub-directory, the WEB-INF directory.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:APACHE:SCALLP</td>
<td>This signature detects attempts to exploit a vulnerability in Apache Web servers. Apache improperly calculates required buffer sizes for chunked encoded requests due to a signed interpretation of an unsigned integer value. Attackers may send chunked encoded requests with the unique Host header value “apache-scalp.c.” in the GET request to create a buffer overflow and execute arbitrary code.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>-----------</td>
</tr>
<tr>
<td>HTTP:AUDIT:MSNG-HTTP-VER</td>
<td>This protocol anomaly is an HTTP request with no version number after the <code>HTTP/...</code>. This may indicate command line access to an HTTP server.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:AUDIT:UNKNOWN-REQ</td>
<td>This protocol anomaly is an unknown HTTP request. Known requests are OPTION, GET, HEAD, POST, PUT, DELETE, TRACE, and CONNECT.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:BADBLUE:INVALID-GET-DOS</td>
<td>This signature detects denial-of-service attempts against Working Resources BadBlue Web server. Attackers may send a maliciously crafted HTTP GET request to the Web server to disable the daemon and render it unusable until restarted.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:BADBLUE:PROXY-RELAY</td>
<td>This signature detects attempts to relay a web request through a BadBlue web server. When BadBlue is using its default configuration, attackers may use the web server as a proxy server to attack internal targets or mask attack activity.</td>
<td>medium</td>
<td>sos5.1.0, sos5.0.0</td>
</tr>
<tr>
<td>HTTP:BIGBROTHER:DIR-TRaversal</td>
<td>This signature detects attempts to view files on the Web server using the BigBrother bb-hist.sh history browser script. Attackers may view any files on the Web server that are accessible to the user the history browser script is running under.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:CGI:ALTAVISTA-TRaversal</td>
<td>This signature detects attempts to exploit a vulnerability in the AltaVista Search engine. The search engine sets up a Web server at port 9000 that listens for search queries. The search function accepts a single <code>../</code> string in the query, providing access to the parent, or <code>http</code> directory. This directory typically contains administrative documents that may include the password for the remote administration utility, which is base-64 encoded. Attackers may send multiple <code>../</code> strings in hex code (ie.<code>%2e%2e%2f</code>) in a query to access the remote administration utility password and gain full remote administration abilities.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:CGI:ANYFORM-SEMICOLON</td>
<td>This signature detects attempts to exploit the AnyForm CGI script, a popular CGI form designed to support simple forms that deliver responses via email. Some versions of AnyForm did not perform user supplied data sanity checking, and may allow remote execution of arbitrary commands on the server.</td>
<td>high</td>
<td>sos5.1.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:CGI:APPLE-QT-FIELDISC1</td>
<td>This signature detects attempts to exploit a vulnerability in Apple QuickTimer Streaming Server. QuickTime Streaming Server v4.1.1 and earlier versions are vulnerable. Attackers may send a maliciously crafted URL to parse_xml.cgi to view files that are not usually accessible through HTTP.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:CGI:AXIS-ACCOUNT</td>
<td>This signature detects a request to an Axis Video Server containing parameters designed to create an Administrator account on the server.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:CGI:BNB-SURVEY-REMOTE-EXEC</td>
<td>This signature detects attempts to access the BNBSurvey survey.cgi program. Attackers may remotely execute commands via shell metacharacters.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:CGI:BUGZILLA-SEMICOLON</td>
<td>This signature detects shell access attempts to exploit the process_bug.cgi script vulnerability in Bugzilla. Attackers may send a semi-colon as an argument to the script, followed by arbitrary shell commands.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>-----------</td>
</tr>
<tr>
<td>HTTP:CGI:DCFORUM-AZ-EXEC</td>
<td>This signature detects shell attempts to exploit the dcenterforum.cgi script in DCForum DC Forum (all versions), which is used to manage web-based discussion boards. Attackers may use maliciously crafted URL requests with the pipe and newline characters to execute arbitrary scripts on the Web server.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:CGI:FORMMAIL-ENV-VAR</td>
<td>This signature detects access to the FormMail CGI program. Attackers may use this program to remotely execute commands.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:CGI:HASSENG-DIR-TRAVERSAL</td>
<td>This signature detects attempts to exploit a vulnerability in the Hassen shopping cart script shop.cgi. Attackers may access arbitrary system files.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:CGI:HTDIG-INCLUSION</td>
<td>This signature detects attempts to exploit a vulnerability in ht://dig, a Web content search engine for UNIX. Because ht://dig improperly validates form input, attackers may pass a maliciously crafted variable to the htsearch CGI script to read files accessible to the program user.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:CGI:HYPERSEEK-DIR-TRAVERSAL</td>
<td>This signature detects attempts to exploit a vulnerability in hxs.cgi, which ships as part of iWeb Hyperseek 2000. Attackers may view arbitrary files and directories.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:CGI:IKONBOARD-BADCOOKIE</td>
<td>This signature detects attempts to exploit a vulnerability in IkonBoard, a popular Web-based discussion board. Attackers may send a maliciously crafted cookie that contains illegal characters to IkonBoard to execute arbitrary code with IkonBoard privileges (typically user level).</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:CGI:INFO2WWW-EXEC</td>
<td>This signature detects attempts to exploit a vulnerability in the info2www CGI script. Attackers may execute arbitrary binaries on the Web server.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:CGI:INFOSRCH-REMOTE-EXEC</td>
<td>This signature detects attempts to exploit a vulnerability in the infosrch.cgi script. Attackers may execute commands on the Web server.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:CGI:LIBCGI-RFP-OVERWRITE</td>
<td>This signature detects attempts to exploit a vulnerability in LIB CGI. Attackers may inject maliciously crafted C code into LIB CGI applications to overwrite the Frame Pointer and execute arbitrary code on the host.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:CGI:MOREOVER-CACHE-FEED</td>
<td>This signature detects attempts to exploit a vulnerability in the cached_feed.cgi script provided by moreover.com. Attackers may view arbitrary system files that are readable by the HTTPd process.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:CGI:TECHNOTE-MAIN-DCLSR</td>
<td>This signature detects directory traversal attempts that exploit the main.cgi script in TECH-NOTE 2000. Because the script validates input incorrectly, attackers may remotely access arbitrary files from the server.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:CGI:TECHNOTE-PRINT-DSCLSR</td>
<td>This signature detects directory traversal attempts that exploit the print.cgi script in TECH-NOTE 2000. Because the script validates input incorrectly, attackers may remotely access arbitrary files from the server.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:CGI:W3-MSQL-CGI-OF</td>
<td>This signature detects attempts to exploit a vulnerability in W3-ssql, a CGI program that acts as a Web interface for Mini SQL (mSQL). W3-ssql version 2.0.11 is vulnerable. Attackers may remotely send a maliciously crafted scanf call to overflow the content-length field and execute arbitrary code with Web server privileges.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>------------</td>
</tr>
<tr>
<td>HTTP:CGI:W3-MSQL-FILE-DISCLSR</td>
<td>This signature detects buffer overflow attempts that exploit the w3-msql CGI script in mini-SQL. Attackers may execute arbitrary commands on the server.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:CGI:WEBPALS-EXEC</td>
<td>This signature detects attempts to exploit a vulnerability in the WebPALS CGI script. Attackers may remotely execute arbitrary code with root permissions.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:CGI:WEBSPEED-WSADMIN</td>
<td>This signature detects attempts to gain administrative access to the WebSpeed server without normal authentication.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:CGI:WEBSPIRS-FILE-DISCLSR</td>
<td>This signature detects attempts to exploit a vulnerability in the SilverPlatter WebSPIRS webspirs.cgi file. Attackers may access arbitrary system files</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:CGI:YABB-DIR-TRAVERSAL</td>
<td>This signature detects attempts to exploit a vulnerability in the YaBB.pl CGI script. Attackers may view arbitrary files.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:CHKP:AUTH-FMT-STR</td>
<td>This signature detects attempts to exploit a vulnerability in some Web servers and Web proxies. Attackers may send user authentication that includes format strings to crash the proxy engine, creating a denial-of-service (DoS) or enabling the attackers to take control of the firewall as root.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:CHKP:FW1-FORMAT-STR</td>
<td>This signature detects attempts to exploit a vulnerability in the CheckPoint AI/Smart Defense HTTP proxy engine. Attackers may send a scheme that includes format strings to crash the proxy engine, creating a denial-of-service (DoS) or enabling the attackers to take control of the firewall as root.</td>
<td>critical</td>
<td>sos5.1.0, sos5.0.0</td>
</tr>
<tr>
<td>HTTP:CHKP:FW1-PROXY</td>
<td>This signature detects attempts to exploit the web proxy functions of CheckPoint FireWall-1. When the HTTP CONNECT method, used to build generic Transit Layer Security over HTTP, is used by default, the firewall web proxies may be used as open TCP proxies. Attackers may use an HTTP proxy to connect to a server, then use the CONNECT method to access other servers and launch further attacks.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:CISCO:IOS-ADMIN-ACCESS</td>
<td>This signature detects attempts to exploit a vulnerability in Cisco IOS. Attackers may remotely gain full administrative access to the router.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:CISCO:VOIP:PORT-INFO-DOS</td>
<td>This signature detects attempts to exploit a vulnerability in Cisco VoIP phones. Versions CP-7910 and later are vulnerable. Attackers may send an arbitrarily long (120000+) StreamID to the PortInformation script to cause an error message that displays a memory dump. Attackers may use this information to reconstruct the calling patterns of a particular phone.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:CISCO:VOIP:STREAM-ID-DOS</td>
<td>This signature detects denial-of-service (DoS) attempts against Cisco VoIP phones. Versions CP-7910 and later are vulnerable. Attackers may send an arbitrarily long (120000+) StreamID to the StreamingStatistics script to cause the phone to reset, creating a DoS for 30 seconds (or until the phone reboots).</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:COLDFUSION:EXPRCALC-OPNFIL</td>
<td>This signature detects attempts to exploit a vulnerability in the ColdFusion ExprCalc.cfm script. Attackers may delete files from a Web server.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>-------------------</td>
</tr>
<tr>
<td>HTTP:COLDFUSION:HEADER-LOG-OF</td>
<td>This signature detects attempts to exploit a vulnerability in the JRun component of Macromedia ColdFusion web server. Attackers may send overly long HTTP headers to overflow the logging function, enabling an attacker to crash or take control of the web server.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:COLDFUSION:JRUN-SC-PARSE</td>
<td>This signature detects attempts to exploit a vulnerability in the JRun component of Macromedia ColdFusion web server. Attackers may pass a semi-colon character to JRun to expose the script source code and other sensitive files.</td>
<td>low</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:DIR:CRYSTAL-REPORTS</td>
<td>This signature detects attempts to exploit a vulnerability in Microsoft Crystal Reports. Users of Visual Studio .NET 2003, Outlook 2003 with Business Contact Manager, or Microsoft Business Solutions Customer Relationship Management (CRM) 1.2 are affected. Attackers may send a malformed URL to the server to read or write to any file on the server.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:DIR:DEEP-PARAM-TRAVERSE</td>
<td>This signature detects directory traversal attempts within HTTP GET or POST form parameters that extend three or more directories. Attackers may exploit a poorly-written CGI program to access or modify private files.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:DIR:PARAM-TRAVERSE</td>
<td>This signature detects directory traversal attempts within HTTP GET or POST form parameters. Attackers may exploit a poorly-written CGI program to access or modify private files.</td>
<td>low</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:DIR:TRVERSE-DIRECTORY</td>
<td>This protocol anomaly is an HTTP directory traversal attempt, i.e. ../../ or ../../../. This may indicate an attempt to evade an IDS (DI is not vulnerable). Note that some websites refer to directories in a way that looks like a traversal.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:EXPLOIT:AMBIG-CONTENT-LEN</td>
<td>This protocol anomaly is an HTTP request that has a Content-Length and Transfer-Encoding header. RFC-2616#4.4 specifies that only one of these two headers should be used in an HTTP request.</td>
<td>low</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:EXPLOIT:BLAZIX-JSPVIEW</td>
<td>This signature detects attempts to exploit a vulnerability in the Blazix, a Java-based Web server. Blazix 1.2 and earlier versions are vulnerable. Because Blazix does not strip bad characters (such as '+' and '*') from URL requests, attackers may send a malicious URL to the Web server to view the jsp server side scripts.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:EXPLOIT:BRUTE-FORCE</td>
<td>This protocol anomaly is too many authentication failures (Web pages that require authentication) within a short period of time between a unique pair of hosts.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:EXPLOIT:BRUTE-SEARCH</td>
<td><strong>This protocol anomaly is multiple 301 (Moved Permanently), 403 (Forbidden), 404 (Not Found) and 405 (Method Not Allowed) errors between a unique pair of hosts within a short period of time. This could indicate that a search robot or a script is methodically searching a Web site for vulnerable directories or CGI scripts. The default maximum number of 301/403/404/405 errors is 16.</strong></td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:EXPLOIT:IE-ZONE-SPOOF</td>
<td>This signature detects attempts to access potentially malicious Web sites. When using Microsoft Internet Explorer, a user can be tricked into visiting a malicious Web site that they believe is benign. Additional IE vulnerabilities may allow the malicious Web site to run scripts in the Local Computer zone, which bypasses security checks on the user’s machine. In your logs for the event, the malicious Web site appears as the destination IP address.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>-----------------</td>
</tr>
<tr>
<td>HTTP:EXPLOIT:ILLEGAL-HOST-CHAR</td>
<td>This signature detects illegal characters in a Host header field of an HTTP/1.1 request. Attackers may send an HTTP link, that, when selected by the user, generates an HTTP request to a malicious Web site. In your logs, the destination IP address for the event may be the malicious Web site; however, some foreign Web sites may also trigger this signature, creating a false positive. Per RFC, '_' is not a legal character for a host name.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:EXPLOIT:REALPLAYER-SKIN</td>
<td>This signature detects malicious RealPlayer skin files.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:EXPLOIT:SHOUTCAST-FMT-STR</td>
<td>This signature attempts to exploit a known vulnerability in the Shoutcast streaming audio server. Attackers may gain complete control of the target host.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:EXPLOIT:WIN-MAL-COMP-FILE</td>
<td>This signature detects attempts to exploit a vulnerability in Microsoft Windows native compressed file handler. Attackers may send.zip files with overly long filenames to overflow the file handler and run arbitrary code.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:EXT:GRP-EXT-HTTP</td>
<td>This signature detects GRP files sent over HTTP. GRP files can contain Windows Program Group information, and may be exploited by malicious users to deposit instructions or arbitrary code on a target’s system. User involvement is required to activate GRP files; typically they are attached or linked to a harmless-appearing e-mail message.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:EXT:JOB</td>
<td>This signature detects an attempt to download a Microsoft Task Scheduler (.job) file. Opening a malicious .job file in Task Scheduler may allow for arbitrary code execution, leading to system compromise. This vulnerability is present in Microsoft Windows 2000 Service Pack 2 and later. It is also present in Microsoft Windows XP Service Pack 1.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:FRONTPAGE:ADMIN.PWD-REQ</td>
<td>This signature detects attempts to access the Microsoft FrontPage Extensions for UNIX .pwd file that contains sensitive account information.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:FRONTPAGE:DOS-NAME-DOS</td>
<td>This signature detects attempts to exploit a known vulnerability in Microsoft Frontpage. Attackers may send a malformed request with an MS-DOS device name to shtml.exe to crash the server.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:FRONTPAGE:FOURDOTS</td>
<td>This signature detects attempts to exploit the ‘../...’ directory traversal vulnerability in Microsoft FrontPage PWS.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:FRONTPAGE:FP30REG.DLL-OF</td>
<td>This signature detects buffer overflow attempts against Microsoft FrontPage extensions in Windows 2000 and XP. Attackers may execute arbitrary code on the target host.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:FRONTPAGE:SERVICE.PWD-REQ</td>
<td>This signature detects attempts to access the Microsoft FrontPage extensions for UNIX .pwd file which contains sensitive account information.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:HOSTCTRL: BROWSE-ASP</td>
<td>This signature detects attempts to exploit a vulnerability in the browse.asp script supplied with Hosting Controller, a tool that allows Microsoft Windows network administrators to centralize administrative tasks into one interface. Attackers may send a maliciously crafted URL request for browse.asp to view arbitrary directories and files on hard drives.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:HOTMAIL:EXE-DOWNLOAD</td>
<td>This signature detects attempts by users to download potentially hazardous attachments from MSN Hotmail.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>--------------</td>
</tr>
<tr>
<td>HTTP:IIS:AD-SERVER-CONFIG</td>
<td>This signature detects attempts to download the site.csc configuration file for Microsoft Ad Server. Attackers may access sensitive information.</td>
<td>medium</td>
<td>sos5.0.0,</td>
</tr>
<tr>
<td></td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:IIS:ASP-CODEBROWSER-EXAIR</td>
<td>This signature detects attempts to exploit the Showcode ASP vulnerability in Microsoft IIS.</td>
<td>medium</td>
<td>sos5.0.0,</td>
</tr>
<tr>
<td></td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:IIS:ASP-DOT-NET-BACKSLASH</td>
<td>This signature detects backslash () characters in the URL portion of an HTTP request. Attackers may use a backslash as a directory separator instead of the normal forward slash (/) to bypass the Microsoft IIS ASP.Net authentication capabilities and access protected resources. Note: A poorly configured web server may also display a backslash in a non-malicious URL request.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:IIS:BAT-&amp;</td>
<td>This signature detects attempts to execute a command by specifying a .bat or .cmd extension to a Microsoft Windows Web server.</td>
<td>high</td>
<td>sos5.0.0,</td>
</tr>
<tr>
<td></td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:IIS:COMMAND-EXEC</td>
<td>This signature detects attempts to exploit Microsoft Windows Web servers. Attackers may send a maliciously crafted url containing the string &quot;cmd.exe&quot; to execute commands on the Web server.</td>
<td>medium</td>
<td>sos5.0.0,</td>
</tr>
<tr>
<td></td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:IIS:COMMAND-EXEC-2</td>
<td>This signature detects attempts to exploit a vulnerability in Microsoft IIS. Attackers may execute arbitrary commands on the Web server.</td>
<td>high</td>
<td>sos5.0.0,</td>
</tr>
<tr>
<td></td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:IIS:DATA-DISCLOSURE</td>
<td>This signature detects attempts to obtain the sourcecode of Active Server Pages served by Microsoft's Internet Information Server. In IIS, remote attackers can obtain source code for ASP files by appending &quot;::$DATA&quot; to the URL.</td>
<td>high</td>
<td>sos5.0.0,</td>
</tr>
<tr>
<td></td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:IIS:HEADER-HOST-DOS</td>
<td>This signature detects denial-of-service (DoS) attempts against Microsoft IIS. Attackers may pass maliciously malformed header values to the host to crash the IIS service.</td>
<td>high</td>
<td>sos5.0.0,</td>
</tr>
<tr>
<td></td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:IIS:NSISISLOG-OF</td>
<td>This signature detects buffer overflow attempts against Microsoft Windows Media Services, included with Microsoft Windows 2000 Server SP4. Attackers may send a maliciously crafted HTTP &quot;POST&quot; request to overflow the buffer.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:IIS:ISAPI-IDA-OVERFLOW</td>
<td>This signature detects buffer overflow attempts against Microsoft ISAPI Indexing Service for IIS. Index Server 2.0 and Indexing Service 2000 in IIS 6.0 beta and earlier versions are vulnerable. Attackers may send a long argument to Internet Data Administration (.ida) and Internet Data Query (.idq) files to overflow the buffer in the ISAPI extension (idq.dll) and execute arbitrary commands.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:IIS:ISAPI-IDQ-OVERFLOW</td>
<td>This signature detects buffer overflow attempts against Microsoft ISAPI Indexing Service for IIS. Index Server 2.0 and Indexing Service 2000 in IIS 6.0 beta and earlier versions are vulnerable. Attackers may send a long argument to Internet Data Administration (.ida) and Internet Data Query (.idq) files to overflow the buffer in the ISAPI extension (idq.dll) and execute arbitrary commands.</td>
<td>critical</td>
<td>sos5.1.0,</td>
</tr>
<tr>
<td></td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
<td>sos5.0.0</td>
</tr>
<tr>
<td>HTTP:IIS:ISAPI-PRINTER-OVERFLOW</td>
<td>This signature detects attempts to execute a buffer overflow in the Microsoft IIS 5.0 .printer ISAPI extension.</td>
<td>critical</td>
<td>sos5.0.0,</td>
</tr>
<tr>
<td></td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:IIS:MALFORMED-HTR-REQUEST</td>
<td>This signature detects malformed .htr requests that may cause a denial-of-service (DoS).</td>
<td>high</td>
<td>sos5.0.0,</td>
</tr>
<tr>
<td></td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------------</td>
</tr>
<tr>
<td>HTTP:IIS:MDAC-RDS</td>
<td>This signature detects attempts to exploit the Microsoft Data Access Components (MDAC) Remote Data Services (RDS) component. Attackers may access files and other services.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:IIS:MDAC-RDS-2</td>
<td>This signature detects attempts to exploit the Remote Data Services (RDS) component included in Microsoft Data Access Components (MDAC) using ActiveDataFactory. Microsoft IIS 3.x and 4.x are vulnerable. Attackers may remotely access exposed unsafe methods to execute arbitrary commands.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:IIS:MFC-EXT:OF</td>
<td>This signature detects buffer overflow attempts against Microsoft IIS. A maliciously crafted HTTP request can exploit a buffer overflow condition in mfc42.dll by way of ext.dll. Attackers may gain local access to an IIS server.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:IIS:NEWDSN-FILE-CREATION</td>
<td>This signature detects attempts to create a file on the Web server by exploiting the newdsn.exe vulnerability in Microsoft IIS 3.0.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:IIS:NSISLOG-CHUNKED-POST</td>
<td>This signature detects chunked POST requests to NSISLOG.DLL. Attackers may exploit Windows Media Services that have logging enabled, and other vulnerabilities using this method.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:IIS:OUTLOOK-WEB-DOS</td>
<td>This signature detects denial-of-service (DoS) attempts against Microsoft Outlook Web. Attacker may send a long string of '%' characters as the user name and/or password.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:IIS:PROPFIND</td>
<td>This signature detects attempts to exploit a vulnerability in Microsoft IIS 5.0. Attackers may send malicious 'PROPFIND' requests to the server to crash it.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:IIS:SADMIND-WORM-ACCESS</td>
<td>This signature detects the sadmind/IIS worm attempting to infect Microsoft IIS. The sadmind/IIS worm first exploits a vulnerability in a Solaris system, then attacks Microsoft IIS Web servers using the Web server folder directory traversal exploit.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:IIS:SENSEPOST.EXE</td>
<td>This signature detects attempts to locate sensepost.exe on a Microsoft ISS Web Server. Attackers may use a proof-of-concept hacking tool to break into a vulnerable Web server, then copy cmd.exe to the Web server script directory and rename it sensepost.exe to avoid detection by log viewers. To identify this event, check your Web server logs for details—if the server returned a '200' to the request, your Web server may be compromised.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:IIS:SITEM-SERVER-FILE-UPLD</td>
<td>This signature detects attempts to exploit a vulnerability in MS Site Server 2.0 with IIS 4. Attackers may upload content (including ASP) to the target web site and remotely execute commands.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:IIS:WEBDAV:LOCK-OF</td>
<td>This signature detects buffer overflow attempts against Microsoft IIS WebDAV. Attackers may send a maliciously crafted WebDAV URL request that contains 65535 or 65536 bytes to the Web server to execute arbitrary code as the system account.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:IIS:WEBDAV:MALFORMED-REQ1</td>
<td>This signature detects denial-of-service (DoS) attempts against Microsoft IIS 5.0 servers with WebDAV extensions enabled. Attackers may send a maliciously crafted WebDAV SEARCH request in an HTTP request to DoS the Web server.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>------------</td>
</tr>
<tr>
<td>HTTP:IIS:WEBDAV:MALFORMED-REQ2</td>
<td>This signature detects denial-of-service (DoS) attempts against Microsoft IIS 5.0 servers with WebDAV extensions enabled. Attackers may send a maliciously crafted WebDAV SEARCH request in an HTTP request to DoS the Web server.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:IIS:WEBDAV:SEARCH-OF</td>
<td>This signature detects buffer overflow attempts against Microsoft IIS WebDAV. Attackers may send a maliciously crafted WebDAV URL request that contains 65535 or 65536 bytes to the Web server to execute arbitrary code as the system account.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:IIS:WEBDAV:XML-HANDLER-DOS</td>
<td>This signature detects denial-of-service (DoS) attempts against the WebDAV XML Message Handler in Microsoft IIS. Attackers may send a malicious HTTP request to a WebDAV enabled IIS server to cause it to consume all system resources. A machine reboot is required to resume service.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:INFO:HTTPPOST-GETSTYLE</td>
<td>This signature detects HTTP POST requests with GET parameters. POST requests should not have parameters on the same line as the request method. This may indicate a poorly-written Web application or HTTP tunneling.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:INFO-LEAK:GOAHEAD-PERM</td>
<td>&quot;This signature detects attempts to bypass directory permissions set on the /cgi-bin directory of a GoAhead web server. GoAhead WebServer versions 2.1.8 and earlier are vulnerable. Attackers may supply an invalid URL to the server to reveal the contents of certain private directories on the server.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:INFO-LEAK:HTACCESS</td>
<td>This signature detects probes for the .htaccess file, used by the Apache Web server for configuration directives. Attackers may be attempting to gain access to the Web server.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:INFO-LEAK:HTPASSWD-REQUEST</td>
<td>This signature detects attempts to access the .htpasswd file on a Web server.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:INFO-LEAK:VIGNETTE-DIAG</td>
<td>This signature detects attempts to access the diagnostic utility supplied with the Vignette Application server. Because the utility does not use access controls, attackers (or any client) may connect to the utility and access sensitive configuration information.</td>
<td>low</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:INFO-LEAK:VIGNETTE-LEAK</td>
<td>&quot;This signature detects attempts to exploit a vulnerability in Vignette Story Server. Vignette Story Server versions 4.1 and 6 are vulnerable. Attackers may expose information about user sessions, server side code, and other sensitive information.</td>
<td>low</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:INFO-LEAK:WEB-INF-DOT</td>
<td>This signature detects attempts to exploit a vulnerability in Windows Web servers with J2EE. Attackers may append a '.' character to a request for the WEB-INF directory (where J2EE class files are typically stored) to bypass directory security and gain access to normally protected files.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:INFO-LEAK:WR850-CONF-DL</td>
<td>This signature detects attempts to download the configuration file from a Motorola WR850G Wireless Router.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:INVALID:INVLD-AUTH-CHAR</td>
<td>This protocol anomaly is an HTTP header with an authorization string that contains an invalid character. The authorization line is decoded using base64.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>-----------</td>
</tr>
<tr>
<td>HTTP:INVALID:INVALID-AUTH-LEN</td>
<td>This protocol anomaly is an HTTP header with an authorization string that has an invalid length (a length that is not a multiple of 4). Because the authorization line is encoded/decoded using base64, the length must be a multiple of 4.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:INVALID:MISSING-REQ</td>
<td>This protocol anomaly is an HTTP header that has no request line or request uniform resource identifier (URI).</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:IRIX:CGI-BIN-WRAP</td>
<td>This signature detects attempts to exploit the wrap CGI script in SGI IRIX. Attackers may list the contents of Web server directories.</td>
<td>medium</td>
<td>sos5.0.0,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:MISC:EMULIVE-ADMIN</td>
<td>This signature detects an attempt to gain unauthorized administrative access to an EmuLive Server4 daemon.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:MISC:HP-PROCURVE-RESET</td>
<td>This signature detects denial-of-service (DoS) attempts against the HP Procurve 4000M switch. Configuration changes for the switch are made via an HTTP-based interface; however, the script that resets the switch after a configuration change does not properly authenticate the IP address that calls the script. Attackers may call the script repeatedly to perform a DoS.</td>
<td>medium</td>
<td>sos5.0.0,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:MISC:MOBY-LENGTH-DOS</td>
<td>This signature detects denial-of-service (DoS) attacks against the Moby NetSuite. Attackers may send a maliciously crafted HTTP POST request that contains an invalid Content-Length field to the host to crash the Web server.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:MISC:MOODLOGIC-CLIENT</td>
<td>This signature detects use of the Mood Logic client. Mood Logic is an MP3 catalogue system that helps users identify and classify MP3s. If your organization prohibits the use of MP3s, use this signature to detect Mood Logic clients.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:MISC:NG-WG602-BACKDOOR</td>
<td>This signature detects attempts to administer a Netgear WG602 using an undocumented administrator username/password that cannot be changed or disabled. Attackers can modify any setting on the WG602 to perform a denial-of-service (DoS) on the Netgear device or circumvent other access control protocols.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:MISC:NOOP-SLIDE-HEAD-OF</td>
<td>This signature detects buffer overflow attempts against Web servers on Intel x86 platforms. Attackers may use the &quot;No-Op Slide&quot; attack to pad the stack with &quot;No Operation&quot; x86 CPU instructions and overwrite the return address.</td>
<td>critical</td>
<td>sos5.0.0,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:MISC:NOOP-SLIDE-REQ-OF</td>
<td>This signature detects buffer overflow attempts against Web servers on Intel x86 platforms. Attackers may use the &quot;No-Op Slide&quot; attack to pad the stack with &quot;No Operation&quot; x86 CPU instructions and overwrite the return address.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:MISC:SHAMBALA-DOS1</td>
<td>This signature detects denial-of-service (DoS) attempts against Evolvable Shambala Server, an FTP, Web, and Chat server. Version 4.5 is vulnerable. Attackers may send a maliciously crafted request to the Web server to cause a DoS.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:MISC:VISNETIC-DOS</td>
<td>This signature detects attempts to exploit a vulnerability in VisNetic WebSite. Versions 3.5.13.1 and earlier are vulnerable. Attackers may send a malicious OPTIONS request to crash the server.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>--------------</td>
</tr>
<tr>
<td>HTTP:MISC:WR850:WEB SHELL</td>
<td>This signature detects attempts to access a debug mode web shell supplied with the Motorola WR850 Wireless Router. Attackers may use this access exploit in conjunction with an authentication bypass exploit to gain full control over the router.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:NETSCAPE:ENTERPRISE-DOS</td>
<td>This signature detects denial-of-service (DoS) attempts that exploit the Web Publishing REVLOG command in Netscape Enterprise Server 3.x.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:NOVELL:NETWARE-CONVERT.BAS</td>
<td>This signature detects directory traversal attempts on Novell NetWare Web Server 2.x. The convert.bas CGI script allows file retrieval outside of normal Web server context. Attackers may submit the filename and path as a parameter to the script using relative paths (../../) to traverse directories.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OREILLY:WIN-C-SMPLE-OVFLOW</td>
<td>This signature detects buffer overflow attempts that exploit the win-c-sample.exe sample script vulnerability in O’Reilly Website Pro 2.0 Web server. The script is placed in the /cgi-shl directory off of the Web root by default.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:ACCEPT</td>
<td>DI has detected a suspiciously long Accept header.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:ACCEPT-ENCODING</td>
<td>DI has detected a suspiciously long Accept-Encoding header.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:ACCEPT-LANGUAGE</td>
<td>DI has detected a suspiciously long Accept-Language header.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:ATP-HTTPD-OF</td>
<td>This signature detects buffer overflow attempts against ATPhttp versions 0.4b and earlier. Attackers may send an overly long GET request to the Web server daemon to overflow the buffer.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:AUTHORIZATION</td>
<td>This protocol anomaly is an HTTP authorization header that exceeds the user-defined maximum. The default length is 128.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:AUTH-OVFLW</td>
<td>This protocol anomaly is an HTTP header with an authorization line that exceeds the user-defined maximum. The default authorization line length is 128.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:CHUNK-LEN-OFLW</td>
<td>This protocol anomaly is an HTTP message that has a chunk length in a Transfer-Encoding: chunk request that is greater than 0x7fffffff. Apache servers 1.3 to 1.3.24 and 2.0 to 2.0.36 are vulnerable. Attackers may cause a denial-of-service (DoS) or execute arbitrary code on the server.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:CHUNK-OVERFLOW</td>
<td>This protocol anomaly is an invalid data chunk length in an HTTP request that uses chunked encoding. The chunked encoding transfer method sends data length requests followed by data chunks that match the negotiated data lengths. Attackers may cause a stack overflow and execute arbitrary code on the server.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:CONNECTION</td>
<td>DI has detected a suspiciously long Connection header.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:CONTENT-ENCODING</td>
<td>DI has detected a suspiciously long Content-Encoding header.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:CONTENT-LANGUAGE</td>
<td>DI has detected a suspiciously long Content-Language header.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:CONTENT-LENGTH</td>
<td>DI has detected a suspiciously long Content-Length header.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:CONTENT-LOCATION</td>
<td>DI has detected a suspiciously long Content-Location header.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:CONTENT-MD5</td>
<td>DI has detected a suspiciously long Content-MD5 header.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:CONTENT-OVERFLOW</td>
<td>This protocol anomaly is a missing line break after a specified data length in an HTTP request using content length transfer. The content length transfer method sends the specified data length in the BODY of the request followed by a line break.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:CONTENT-TYPE</td>
<td>This protocol anomaly is a Content-Type header length that exceeds the user-defined maximum. The default length is 64.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:COOKIE</td>
<td>This protocol anomaly is an HTTP Cookie header length that exceeds the user-defined maximum. The default length is 8192.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:HEADER</td>
<td>This protocol anomaly is an HTTP header field that is too long, and may indicate a buffer overflow attempt.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:HOST</td>
<td>This protocol anomaly is an HTTP Host header length that exceeds the user-defined maximum. The default length is 64.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:HTTPA-OF1</td>
<td>This signature detects buffer overflow attacks against the HTTPa daemon. Attackers may send a maliciously crafted HTTP GET request to the host to overflow the buffer.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:INV-CHUNK-LEN</td>
<td>This protocol anomaly is an invalid chunk length specification in a chunked transfer encoded HTTP request. RFC-2616#3.6.1 specifies that the size of a chunk should be represented using hexadecimal notation.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:JANASRV-VER-OF</td>
<td>This signature detects buffer overflow attempts against JanaServer HTTP Server, an Internet gateway for Windows. JanaServer 2.21 and prior are vulnerable. Attackers may send a maliciously crafted HTTP GET request to crash the server.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:LIBHTTPD-GET-OF</td>
<td>This signature detects buffer overflow attempts against LibHTTPD. LibHTTPD 1.2 and earlier are vulnerable. Attackers may send a maliciously crafted GET request to execute arbitrary code on the host.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:METHOD-GENRC-OF</td>
<td>This signature detects buffer overflow attempts against HTTP request methods. Attackers may send an invalid or long HTTP request to crash the server.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:NULLHTTPD-ROOT-OF</td>
<td>This signature detects buffer overflow attempts against Null HTTPD. Attackers may remotely send shellcode in a maliciously crafted POST command to gain local access.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:PI3WEB-SLASH-OF</td>
<td>This signature detects denial-of-service (DoS) attempts against PI3Web Server. Attackers may send a URL with more than 354 Slashes (/) to crash the server.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:REFERER</td>
<td>This protocol anomaly is an HTTP Referer header length that exceeds the user-defined maximum. The default length is 8192.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:SAMBAR-SEARCH</td>
<td>This signature detects buffer overflow attempts against Sambar Server, a free Web server. Attackers may include an oversized HTTP header within a maliciously crafted request to the server to execute arbitrary code.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:SERVER</td>
<td>DI has detected a suspiciously long Server header.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:SET-COOKIE</td>
<td>DI has detected a suspiciously long Set-Cookie header.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>------------</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:TRANSFER-ENCODING</td>
<td>DI has detected a suspiciously long Transfer-Encoding header.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:USER-AGENT</td>
<td>This protocol anomaly is an HTTP User-Agent header length that exceeds the user-defined maximum. The default length is 258.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:ALEXPHP-INCLUDE</td>
<td>This signature detects attempts to exploit a remote file inclusion vulnerability in AlexPHP. Attackers may send a maliciously crafted HTTP request to execute PHP code from a remote server on the host running AlexPHP.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:BLACKBOARD-INC</td>
<td>This signature detects attempts to exploit a vulnerability in the admin.inc.php script that shipped as part of the BlackBoard suite. Attackers may force the admin.inc.php script to include and execute PHP code from a remote source.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:COOLPHP-DIRTRA/</td>
<td>This signature detects directory traversal attempts against CoolPHP. Attackers may use this exploit to execute arbitrary scripts on the PHP server.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:DFORUM-PHP-INC</td>
<td>This signature detects attempts to exploit a vulnerability in D-Forum. D-Forum versions 1.0 through 1.11 are vulnerable. Attackers may exploit header.php3 and footer.php3 to include PHP code from a remote host and execute arbitrary commands.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:FI-DIR-TRAVERSAL</td>
<td>This signature detects attempts to exploit a design vulnerability in PHP/FI. Attackers may remotely access files and directories that are readable by the Web server UID to gather information on the local host and retrieve encrypted user passwords on the system.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:GALLERY:EMBED-AUTH</td>
<td>This signature detects attempts to exploit a vulnerability in Gallery, a Web-based photo album application written in php. Attackers may bypass user authorization to gain administrative privileges.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:GALLERY:HTTP-VARS</td>
<td>This signature detects attempts to exploit a vulnerability in Gallery, a Web-based photo management application. Gallery uses the variables HTTP_POST_VARS, HTTP_GET_VARS, HTTP_COOKIE_VARS, and HTTP_POST_FILES to transfer data between pages, including the GALLERY_BASEDIR variable. Attackers may manually control these variables to include a malicious setting for GALLERY_BASEDIR, enabling them to execute arbitrary PHP code on the Gallery server with the permissions of the HTTP server.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:GALLERY:MAL-INCLUDE</td>
<td>This signature detects attempts to exploit a vulnerability in Gallery online photo gallery software. Attackers may inject malicious PHP code into the software to execute operations on the Web server.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:MANTIS-ARB-EXEC1</td>
<td>This signature detects attempts to exploit a vulnerability in Mantis, an open source Web-based bug tracking system. Mantis 0.17.3 and earlier versions are vulnerable. Attackers may send a maliciously crafted URL to cause the Web server to download PHP code from a remote server, allowing the attacker to execute arbitrary code with the permissions of the user that is running the Web server daemon.</td>
<td>medium</td>
<td>sos5.0.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>HTTP:PHP:MANDIS-ARB-EXEC2</td>
<td>This signature detects attempts to exploit a vulnerability in Mantis, an open source Web-based bug tracking system. Mantis 0.17.3 and earlier versions are vulnerable. Attackers may send a maliciously crafted URL to cause the Web server to download PHP code from a remote server, allowing the attacker to execute arbitrary code with the permissions of the user that is running the Web server daemon.</td>
<td>medium</td>
<td>sos5.0.0</td>
</tr>
<tr>
<td>HTTP:PHP:MLOG-SCREEN</td>
<td>This signature detects attempts to exploit the vulnerable mlog.phtml script. Attackers may remotely access arbitrary files on the Web server.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:NULL-CHAR-IN-TAG</td>
<td>This signature detects attempts to exploit a known vulnerability in the PHP Hypertext Processor (PHP) scripting language used on many Unix/POSIX-based web servers. PHP does not properly check for an encoded NULL character (%00) within parameters passed to it. Because PHP does not properly filter the HTML for malicious content, attackers may post HTML that contains malicious code to a PHP-enabled web site. When other users visit the web site, the malicious code runs on their web browser with credentials allowed for the site by that user.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:PHORUM:ADMIN-PW-CHG</td>
<td>This signature detects attempts to exploit the vulnerable admin.php3 script in Phorum. Attackers may remotely send a maliciously crafted string to the script, change the administrative password of the board without user verification, and access restricted files on the local system.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:PHORUM:READ-ACCESS</td>
<td>This signature detects access to the vulnerable read.php3 script installed with Phorum. Because the script does not validate input, attackers may execute arbitrary SQL statements to modify the database contents, insert new entries, create and drop tables, etc.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:PHORUM:REMOTE-EXEC</td>
<td>This signature detects attempts to exploit a vulnerability in the PHP Phorum bulletin board system. Attackers may remotely execute arbitrary commands with the privileges of the HTTP server.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:PHPBB:HIGHLIGHT-EXEC</td>
<td>This signature detects attempts to exploit a vulnerability in phpBB. Attackers may send a malformed HTTP request to phpBB to force phpBB to execute arbitrary perl commands on the server with Web server permissions.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:PHPBB:HIGHLIGHT-EXEC2</td>
<td>This signature detects attempts to exploit a vulnerability in phpBB. Attackers may send a malformed HTTP request to phpBB to force phpBB to execute arbitrary perl commands on the server with Web server permissions.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:PHPBB:PM_SQL_USR</td>
<td>This signature detects attempts to inject SQL code into a request to phpBB, a popular open-source bulletin board application written in php. Attackers may send a maliciously crafted request that supplies SQL commands to the pm_sql_user parameter, changing database values and escalating client privileges.</td>
<td>low</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:PHPBB:SEARCH-INJECT</td>
<td>This signature detects attempts to exploit a vulnerability in phpBB, an open-source bulletin board package. The search_id parameter in phpBB is vulnerable to SQL injection. Attackers may query private data (such as hashed passwords) then embed the password in a cookie to gain administrative access to the Web site.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>HTTP:PHP:PHPDIG-FILE-INC</td>
<td>This signature detects attempts to exploit a vulnerability in PhpDig 1.6. Attackers may include a malicious 'relative_script_path' parameter in a direct request to the config.php script; this request causes the server to download php code from remote location and execute it. Attackers may execute arbitrary code on the server with permissions of the web server.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:PHPLIB-REMOTE-EXEC</td>
<td>This signature detects attempts to exploit a vulnerability in PHPLIB, a code library that provides support for managing sessions in Web applications. Attackers may remotely submit maliciously crafted Web requests to cause the application to fetch and execute scripts from another host, allowing local access to the Web server.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:PHPMYADMIN:SVR-PARAM</td>
<td>This signature detects attempts to exploit a vulnerability in PHPMyAdmin. Attackers may use HTTP form parameters to remotely provide mysql server configuration data. This attack is typically one stage in a multi-stage exploit attempt.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:PHPNuke:CID-SQL-INJECT</td>
<td>This signature detects attempts to exploit a vulnerability in PHP-Nuke. Attackers may execute arbitrary SQL commands on a Web server.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:PHPNuke:MODULES-DOS</td>
<td>This signature detects attempts to exploit a SQL injection vulnerability in the modules.php script that ships with PHPNuke. PHPNuke 6.0 and earlier are vulnerable. Attackers may produce a process that increases system load on the server, making it unusable until the process is killed.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:PHPROJEKT-INC</td>
<td>This signature detects attempts to exploit a vulnerability in the authform.inc.php script included in the PHProjekt package. Attackers may supply a remote location in the 'path_pre' input parameter to force the target to download and execute arbitrary PHP code from the remote location.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:PHPWEB-REMOTE-FILE</td>
<td>This signature detects attempts to exploit a vulnerability in phpWebsite. Version 0.8.2 and earlier are vulnerable. Attackers may specify a remote file location for file inclusion to cause phpWebsite to execute arbitrary PHP code; attackers may execute commands with HTTP daemon user permissions.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:PMACHINE-INCLUDE</td>
<td>This signature detects attempts to exploit a vulnerability in pMachine, an online publishing application. pMachine version 2.2.1 and other versions are vulnerable. Attackers may send a malicious HTTP request to force the pMachine Web server to execute PHP code from a remote server; commands are executed with web server privileges.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:POPPER-OPEN-ADMIN</td>
<td>This signature detects attempts to exploit a vulnerability in popper_mod 1.2.1, a Web-based PHP POP3 email client based on Qpopper. Popper_mod relies on htaccess authentication to authenticate administrators; if htaccess is not used to protect admin access, popper_mod does not authenticate administrators. Attackers may browse to the /mail/admin directory to access the administration PHP script and view a complete list of user accounts and passwords, delete accounts, modify accounts, and edit settings.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>---------------</td>
</tr>
<tr>
<td>HTTP:PHP:REDHAT-PIRANHA-PASSWD</td>
<td>This signature detects attempts to exploit the vulnerable passwd.php script in the Piranha virtual server package (RedHat Linux 6.2). Because the script does not validate input properly, attackers may authenticate to the Piranha package with the effective ID of the Web server and execute arbitrary commands.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:SILENT-STORM-ADMIN</td>
<td>This signature detects attempts to raise the privileges on an account for the Silent Storm PHP Portal.</td>
<td>low</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:UPLOAD-LOCATION</td>
<td>This signature detects a maliciously crafted HTTP POST request. Attackers may use a directory traversal attack within the Content-Disposition field of a POST request to force PHP to execute arbitrary code.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:VBULL-CAL-EXEC</td>
<td>This signature detects attempts to exploit a vulnerability in the calendar.php script that is included with the VBulletin package. Attackers may run the vbull.c exploit to execute arbitrary commands with Web Server user permissions.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:WOLTAB-SQL-INJ</td>
<td>Any user on the bulletin board can compromise any other user's account by exploiting a vulnerability in board.php. Board.php does not perform proper input validation, and therefore is subject to executing user-supplied SQL statements. This is known to affect Woltab Burning Board 2.0 RC 1 and earlier versions.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:YABBSE-PKG-EXEC</td>
<td>This signature detects attempts to exploit a vulnerability in Packages.php in YabbSE. YabbSE 1.5.0 and earlier are vulnerable. Attackers may include remote malicious code in Packages.php to include remote malicious code to execute arbitrary commands with Web server privileges.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:YABBSE-SSI-INCLUDE</td>
<td>This signature detects attempts to exploit a vulnerability in YabbSE, a PHP/MySQL port of the forum software YaBB (yet another bulletin board). YabbSE versions 1.5.2 and earlier are vulnerable. Attackers may include PHP code in a maliciously crafted URL request; when YabbSE receives the request it runs the PHP code, enabling the attacker to execute arbitrary commands on the server.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:ZENTRACK-CMD-EXEC</td>
<td>This signature detects attacks against the PHP-based zenTrack CRM system. A vulnerability exists in the header.php that holds zenTrack configuration settings. It allows remote command execution as the webserver process privilege. This applies to zenTrack 2.4.1 and below.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PKG:ALLAIRE-JRUN-DOS</td>
<td>This signature detects an attempt to launch a denial-of-service (DoS) attack in Allaire JRun 3.0/3.1. Attackers may send a long string of <code>:</code> characters after the /servlet/ prefix in the URL to cause the server to interpret the URL as a very large tree of non-existent directories and to consume system resources.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PKG:DB4WEB-FILE-ACCESS-LIN</td>
<td>This signature detects attempts to exploit a vulnerability in DB4Web (R) Application Server for Windows. Attackers may use a Web browser to download arbitrary files to the target host and obtain system information such as passwords.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PKG:EWAVE-SERVLET-DOS</td>
<td>This signature detects denial-of-service (DoS) against the eWave Servlet JSP. Attackers may remotely send URL requests to cause the Servlet engine to terminate abruptly.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------------</td>
</tr>
<tr>
<td>HTTP:PKG:_MOUNTAIN-ORDR-DSCLSR</td>
<td>This signature detects attempts to exploit a vulnerability in Mountain Network Systems Webcart software. Attackers may remotely execute arbitrary commands on the server.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PKG:WEBGAIS-REMOTE-EXEC</td>
<td>This signature detects attempts to exploit the webserver script in WebGais. Attackers may execute arbitrary commands on the Web server.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PROXY:DOUBLE-AT-AT</td>
<td>This signature detects URLs that contain multiple @ characters. Squid/2.3.STABLE5 is vulnerable. Internet Explorer users may use these malicious URLs to evade web proxies and gain direct access to the internet.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:REQERR:HEADER-INJECT</td>
<td>This signature detects attempts to exploit an input validation vulnerability in HTTP. Attackers may use encoded CR/LF (carriage return/line feed) characters in an HTTP response header to split HTTP responses into multiple parts, enabling them to misrepresent web content to the recipient.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:REQERR:REQ-INVALID-FORMAT</td>
<td>This protocol anomaly is an invalid HTTP request format, such as a request that begins before a previous one ends.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:REQERR:REQ-LONG-UTF8CODE</td>
<td>This protocol anomaly is an HTTP request with an exceedingly long UTF8 codes. This may be an attempt to overflow a portion of the Web server, or that a script is being made available to the Web server.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:REQERR:REQ-MALFORMED-URL</td>
<td>This protocol anomaly is a malformed URL, such as a Unicode encoded field with non-hex digits or an encoded NULL byte.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:SNAVT:GET-DOT1</td>
<td>This signature detects denial-of-service (DoS) attempts against the Savant HTTP server. Savant HTTP server 3.0 and earlier versions are vulnerable. Attackers may send a maliciously crafted HTTP GET request to the Web server to crash the server and create a DoS.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:SPYWARE:DOWNLOAD-ACCEL</td>
<td>This signature detects the use of Download Accelerator, a spyware application.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:SPYWARE:GATOR</td>
<td>This signature detects the use of Gator, a spyware application.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:SPYWARE:NEW-DOT-NET</td>
<td>This signature detects the use of New.net, a spyware application.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:SQL:INJECTION:CMD-CHAIN-1</td>
<td>This signature detects a SQL command sequence in a URL. Because SQL commands are not normally used in HTTP connections, this may indicate a SQL injection attack. However, it may also be a false positive.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:SQL:INJECTION:CMD-CHAIN-2</td>
<td>This signature detects a long SQL command sequence in a URL. Because SQL commands are not normally used in HTTP connections, this may indicate a SQL injection attack.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:SQL:INJECTION:CMD-IN-URL</td>
<td>This signature detects SQL commands within a URL. Because SQL commands are not normally used in HTTP connections, this may indicate a SQL injection attack. However, it may be a false positive.</td>
<td>low</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:SQL:INJECTION:FACTO-CMS</td>
<td>This signature detects attempts to exploit a vulnerability in the FactoSystem Content Management System (CMS). Attackers may introduce instructions into a SQL query to create a non-authorized CMS account.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>HTTP:SQL:INJECTION:GENERIC</td>
<td>This signature detects specific characters, typically used in SQL, within an HTTP connection. Because these characters are not normally used in HTTP, this may indicate a SQL injection attack. However, it may be a false positive. Some attempts at Cross Site Scripting attacks will also trigger this signature.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:SQL:INJECTION:POSTNUKE</td>
<td>This signature detects directory traversal attempts against the modules.php script included with PostNuke. PostNuke versions 0.723 and earlier are vulnerable. Attackers may send a maliciously crafted request to the modules.php to traverse the directory structure and execute SQL queries to the PostNuke database.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:SQL:INJECTION:WS2000</td>
<td>This signature detects SQL injection attempts against a WebStore2000 server. Attackers may inject SQL code into the Item_ID parameter of a maliciously crafted request, enabling them to execute arbitrary SQL commands on the WebStore2000 server.</td>
<td>medium</td>
<td>sos5.1.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:STC:ACROBAT-EXT-OF</td>
<td>This signature detects buffer overflow attempts against Adobe Acrobat Reader. A malicious HTTP server may host an Adobe Acrobat file with an overly long extension; when a client opens this file in Adobe Acrobat Reader, the file triggers a buffer overflow, enabling the server to execute arbitrary code on the client.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:STC:ACROBAT-UUEXEC</td>
<td>This signature detects a maliciously crafted PDF file downloaded via HTTP. Attackers may insert certain shell metacharacters at the beginning of a uuencoded PDF file to force Adobe Acrobat to execute arbitrary commands upon loading the file.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:STC:EICAR-DOWNLOAD</td>
<td>This signature detects the EICAR antivirus test file downloaded via HTTP.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:STC:EXCEL-CELL-OF</td>
<td>This signature detects a maliciously crafted Microsoft Excel file downloaded via HTTP. Attackers may supply an Excel document that contains an overly long Cell Length field to overflow the buffer and execute arbitrary code on the client.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:STC:IE:CONT-LOC-ZON-BYPASS</td>
<td>This signature detects attempts to circumvent a security zone feature that warns when executable files are downloaded. WindowsXP Service Pack 2 and Internet Explorer 6 are vulnerable. Attackers may trick a user into downloading a file that the user did not know was executable. Similarly, viruses and worms may use this method to download themselves onto target computers.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:STC:IE:EXEC-CMD-FILE-SPOOF</td>
<td>This signature detects attempts to exploit a vulnerability in the way that Internet Explorer handles the javascript execCommand function. Attackers may trick a user into saving a file that the user thinks is HTML, but is actually an executable file.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:STC:WINAMP:CDDA-OF</td>
<td>This signature detects the download of a maliciously crafted WinAmp playlist file. Using WinAmp to open this file may execute arbitrary code.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:STC:WINAMP:CDDA-OF2</td>
<td>This signature detects the download of a maliciously crafted WinAmp playlist file. Using WinAmp to open this file may execute arbitrary code.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>HTTP:TOMCAT:JSP-AS-HTML</td>
<td>This signature detects attempts to exploit a vulnerability in Apache Tomcat. Apache Tomcat 3.3.1 and earlier are vulnerable. Attackers may send a maliciously crafted URL to cause the server to parse a .jsp file as HTML code and display the JSP code, allowing attackers to retrieve normally inaccessible files.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:TOMCAT:SERVLET-DEVICE-DOS</td>
<td>This signature detects denial-of-service (DoS) attempts against Apache Group Tomcat Server. Attackers may request a device name from the /examples/servlet directory to render the server inaccessible. This signature also detects attempts to run neuter.c and similar exploits.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:TUNNEL:ALTNET-OVER-HTTP</td>
<td>This signature detects attempts to connect to an AltNet server over HTTP. AltNet is a component of Kazaa, a common Peer to Peer file sharing system. Users may be attempting to download files.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:TUNNEL:CHAT-AOL-IM</td>
<td>This signature detects AOL Instant Messenger Proxy over HTTP. Users may use proxy connections over the HTTP port to circumvent firewall policies.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:TUNNEL:CHAT-MSN-IM</td>
<td>This signature detects MSN Instant Messenger over HTTP. Users may use proxy connections over the HTTP port to circumvent firewall policies.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:TUNNEL:CHAT-YIM</td>
<td>This signature detects Yahoo Instant Messenger Proxy over HTTP. Users may use proxy connections over the HTTP port to circumvent firewall policies.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:TUNNEL:HTTPTUNNEL-URL</td>
<td>This signature detects traffic from the HTTPTunnel utility. HTTPTunnel masquerades a network session in HTTP traffic.</td>
<td>low</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:TUNNEL:KAZAA-OVER-HTTP</td>
<td>This signature detects attempts to connect to a Kazaa server over HTTP. Kazaa is a common Peer to Peer file sharing system. Users may be attempting to download files.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:TUNNEL:SSH</td>
<td>This signature detects SSH over HTTP. Attackers may send SSH over the HTTP port to circumvent firewall policies.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:TUNNEL:TELNET</td>
<td>This signature detects Telnet over HTTP. Attackers may send Telnet over the HTTP port to circumvent firewall policies.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:WASD:CONF-ACCESS</td>
<td>This signature detects attempts to exploit a vulnerability in the WASD HTTP Server for OpenVMS. Default installations of 1.0 and earlier are vulnerable. Attackers may download the configuration file for the server and obtain information on the ACL and internal directory structure.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:WASD:DIR-TRAV</td>
<td>This signature detects directory traversal attempts against WASD HTTP Server for OpenVMS. WASD version 1.0 and earlier are vulnerable. Attackers may navigate to any directory on the server.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:WEBLOGIC:URL-REVEAL-SRC</td>
<td>This signature detects attempts to exploit a vulnerability in Bea Weblogic. Version V6.1 Service Pack 2 on Windows 2000 Server is vulnerable. Attackers may append the string &quot;%00x&quot; to a URL request to read the contents of a .jsp file.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:WEBLOGIC:WEBROOT</td>
<td>This signature detects attempts to exploit a vulnerability in Bea Weblogic. Version V6.1 Service Pack 2 on Windows 2000 Server is vulnerable. Attackers may append the string &quot;%00.jsp&quot; to a normal .html request, causing a compiler error that prints the path to the physical web root.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>-------------------</td>
</tr>
<tr>
<td>HTTP:WEBPLUS:DIR-TRAVERSAL</td>
<td>This signature detects attempts to exploit the input validation vulnerability in the main CGI in TalentSoft Web+, an e-commerce storefront provider. Attackers may pass a script variable that specifies a filepath to the webpsvr daemon, and gain access to any file on the system that the UID of the Web server has access to.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:WEBSPHERE:VER-DOS</td>
<td>This signature detects denial-of-service (DoS) attempts against the caching proxy in IBM WebSphere Edge Server. Version 2.0 is vulnerable. Attackers may send a maliciously crafted HTTP GET request that does not have a proper version identifier to crash the proxy service and render the proxy unusable.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:WIN-CMD:WIN-CMD-EXE</td>
<td>This signature detects the Windows command 'cmd.exe' within a URL. This command does not normally appear in a URL, and may indicate an attempt to compromise the system.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:WIN-CMD:WIN-RGUEST</td>
<td>This signature detects the Windows command 'rguest.exe' within a URL. This command does not normally appear in a URL, and may indicate an attempt to compromise the system.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:WIN-CMD:WIN-WGUEST</td>
<td>This signature detects the Windows command 'wguest.exe' within a URL. This command does not normally appear in a URL, and may indicate an attempt to compromise the system.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:XSS:HDR-REFERRER</td>
<td>This signature detects attempts to exploit a cross-site scripting vulnerability. Attackers may embed malicious HTML tags within the HTTP Referrer header; because some web servers and server-side applications parse this data incorrectly, attackers can successfully execute a cross-site scripting attack.</td>
<td>low</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:XSS:HTML-SCRIPT-IN-URL-PRM</td>
<td>This signature detects attempts at cross site scripting attacks. Attackers may create a malicious Web site that includes HTML embedded in the hyperlinks, which might violate site security settings. Attackers may then view the Web cookies from your computer; Web cookies typically contain sensitive information such as usernames, passwords, credit card numbers, social security numbers, bank accounts, etc.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:XSS:HTML-SCRIPT-IN-URL-PTH</td>
<td>This signature detects cross site scripting attacks. Attackers may create a malicious Web site that includes HTML embedded in the hyperlinks, which might violate site security settings. Attackers may then view the Web cookies from a target computer. Web cookies typically contain sensitive information such as usernames, passwords, credit card numbers, social security numbers, and bank account numbers.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:XSS:URL-IMG-XSS</td>
<td>This signature detects HTML &lt; img&gt; tags in URLs that include Javascript. Because &lt; img&gt; tags should never be present in URLs, the presence of Javascript in such a URL is a clear indication of a Cross-Side Scripting (XSS) attack. XSS attacks are typically Web browser-independent.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>IMAP:FAILURE:BRUTE-FORCE</td>
<td>This protocol anomaly is multiple login failures within a short period of time between a unique pair of hosts.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>IMAP:IPSWITCH:DELE-OF</td>
<td>This signature detects buffer overflow attempts against IPSwitch IMAP server. Attackers may send an overly long delete command (DELE) to overflow the buffer and take complete control of the server.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>IMAP:OVERFLOW:COMMAND</td>
<td>This protocol anomaly is an IMAP command that is too long. This may indicate a buffer overflow attempt.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>IMAP:OVERFLOW:FLAG</td>
<td>This protocol anomaly is an IMAP flag that is too long. This may indicate a buffer overflow attempt.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>IMAP:OVERFLOW:IMAP4-LSUB-OF</td>
<td>This signature detects buffer overflow attempts against the IMAP package included with several Linux distributions. Attackers may send a long string to the IMAP package to execute code with daemon-level permissions.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>IMAP:OVERFLOW:LINE</td>
<td>This protocol anomaly is an IMAP line (from the client to the server) that is too long. This may indicate a buffer overflow attempt. <strong>NOTE:</strong> Long lines are parsed, which may generate other IMAP overflow errors.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>IMAP:OVERFLOW:LIT_LENGTH_OFLOW</td>
<td>This protocol anomaly is an IMAP literal that specifies more octets than the user-defined maximum. A literal is a sequence of zero or more octets. The default maximum number of octets is 65535.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>IMAP:OVERFLOW:MAILBOX</td>
<td>This protocol anomaly is an IMAP mailbox name that is too long. This may indicate a buffer overflow attempt.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>IMAP:OVERFLOW:PASS</td>
<td>This protocol anomaly is an IMAP user password that is too long. This may indicate a buffer overflow attempt.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>IMAP:OVERFLOW:REFERENCE</td>
<td>This protocol anomaly is an IMAP reference field that is too long. This may indicate a buffer overflow attempt.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>IMAP:OVERFLOW:TAG</td>
<td>This protocol anomaly is an IMAP tag field that is too long. This may indicate a buffer overflow attempt.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>IMAP:OVERFLOW:USER</td>
<td>This protocol anomaly is an IMAP user name that is too long. This may indicate a buffer overflow attempt.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>IMAP:REQERR:INVALID_LITERAL_LEN</td>
<td>This protocol anomaly is a literal that specifies a number of octets containing a character that is not 0 or 9.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>IMAP:REQERR:REQ-INVALID-TAG</td>
<td>This protocol anomaly is an invalid IMAP tag, i.e., a tag that begins with a white space or contains non-alphanumeric characters. This may indicate a non-standard IMAP client or command line access to an IMAP server.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>IMAP:REQERR:REQ-UNEXPECTED-ARG</td>
<td>This protocol anomaly is an IMAP command with too many arguments. This may indicate a non-standard IMAP client or command line access to an IMAP server.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
<th>Severity</th>
<th>Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS-RPC:DCOM:SVRNAME-2LONG</td>
<td>This protocol anomaly is a DCOM servername that is longer than 32 octets in unicode.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>MS-RPC:EPDUMP-SCAN</td>
<td>This anomaly detects a client enumerating MSRPC endpoints on a windows server. This may indicate a probing scan prior to a more sophisticated attack.</td>
<td>low</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>MS-RPC:ERR:CL-PTYPE-IN-CO-PDU</td>
<td>This protocol anomaly is an MSRPC connection-oriented message with a packet type that is allowed only in Connectionless PDUs.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>MS-RPC:ERR:CO-PTYPE-IN-CL-PDU</td>
<td>This protocol anomaly is a connectionless MSRPC message with a packet type that is allowed only in connection-oriented PDUs.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>MS-RPC:ERR:EPM-INV-LHS-LEN</td>
<td>This protocol anomaly is an EPM message with an LHS length that is larger than the rest packet length.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>MS-RPC:ERR:EPM-INV-OP-NUM</td>
<td>This protocol anomaly is an invalid EPM operation number.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>MS-RPC:ERR:EPM-INV-RHS-LEN</td>
<td>This protocol anomaly is an EPM message with an RHS length that is larger than the rest packet length.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>MS-RPC:ERR:EPM-INV-TOWER-LEN</td>
<td>This protocol anomaly is an EPM message with a tower length that is larger than 8192 bytes, or larger than the rest fragment length.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>MS-RPC:ERR:EPM-WRONG-LHS-LEN</td>
<td>This protocol anomaly is an EPM packet with a UUID LHS length that is not equal to 19.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>MS-RPC:ERR:EPM-WRONG-RHS-LEN</td>
<td>This protocol anomaly is an EPM message with an RHS length that is larger than the rest packet length.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>MS-RPC:ERR:EPM-WRONG-TOWER-LEN</td>
<td>This protocol anomaly is an EPM message with a tower length that is inconsistent with message’s LHS and RHS lengths.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>MS-RPC:ERR:FRAG-BIGGER-THEN-NEG</td>
<td>This protocol anomaly is a MSRPC fragment length that is larger than the negotiated maximum.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>MS-RPC:ERR:FRAG-LEN-TOO-SMALL</td>
<td>This protocol anomaly is an MSRPC fragment length that is less than the common header length.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>MS-RPC:ERR:INV-AUTH-LEN</td>
<td>This protocol anomaly is an MSRPC message with an authentication length that is larger than the entire MS-RPC message payload length.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>MS-RPC:ERR:INV-AUTH-PAD-LEN</td>
<td>This protocol anomaly is an MSRPC message with authentication padding length plus authentication section length that is larger than the entire MSRPC message payload length.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>MS-RPC:ERR:INV-PTYPE</td>
<td>This protocol anomaly is an MSRPC message that contains an invalid packet type value.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>MS-RPC:ERR:LEN-CONFLICT</td>
<td>This protocol anomaly is an MSRPC connectionless message with a fragment length that conflicts with the common header length and the whole message length.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>MS-RPC:ERR:RESPONSE-NO-REQ</td>
<td>This protocol anomaly is an MSRPC response that precedes the request.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>MS-RPC:ERR:SHORT-MSG</td>
<td>This protocol anomaly is an incomplete MSRPC message.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>MS-RPC:LOC-SVC-OF</td>
<td>This signature detects attempts to exploit a flaw in the Windows DCE RPC Locator service. This service is turned on by default on all Windows NT 4 and Windows 2000 Domain Controllers, or can be turned on manually on all Windows NT, 2000, and XP systems. Attackers can deny the service of the locator, causing network-wide outages, or take control of the service and run code of choice.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>MS-RPC:LSASS:MAL-OPCODE</td>
<td>This signature detects attempts to exploit a known vulnerability in Microsoft Windows LSASS (Local Security Authority Subsystem Service). Attackers may remotely run arbitrary code on the target system. Note: This vulnerability is exploited by many worms.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>MS-RPC:LSASS:OVERSIZED-FRAG</td>
<td>This signature detects attempts to remotely attack a known vulnerability in the Microsoft Windows LSASS (Local Security Authority Subsystem Service). A successful attack could run code of an attacker’s choice on the target system. By supplying an oversized fragment to the LSASS service, a buffer can be overflowed that can result in remote code execution.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>MS-RPC:MSRPC:ISYSACTIVATE-RACE</td>
<td>This protocol anomaly is too many DCE/RPC ISystemActivate requests. Excessive requests can cause a denial-of-service (DoS) in the RPCSS module.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>MS-RPC:NOOP-SLIDE-RPC-REQ</td>
<td>This signature detects Unicode NOOP sleds in an RPC request. Because these patterns are usually malicious, they might indicate an attack.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>MS-RPC:SAMR-ACCESS-DENIED</td>
<td>This signature detects failed attempts to connect to the Security Account Manager Remote (SAMR) service on Windows. Attackers may be probing your server for vulnerabilities, as a successful login to this service provides important information such as administrator account details, default domain names, open users, and active groups. However, because system administrators also use the SAMR service legitimately, this signature may also detect non-malicious activity.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>MS-RPC:SAMR-ACCESS-REQUEST</td>
<td>This signature detects attempts to connect to the Security Account Manager Remote (SAMR) service on Windows. Attackers may be probing your server for vulnerabilities, as a successful login to this service provides important information such as administrator account details, default domain names, open users, and active groups. However, because system administrators also use the SAMR service legitimately, this signature may also detect non-malicious activity.</td>
<td>low</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>MS-RPC:WKST-SVC-OFLOW</td>
<td>This protocol anomaly is a suspiciously long argument for the NetrValidateName, NetrValidateName2, or NetrAddAlternateComputerName functions requested using a named-pipe transaction. An unauthenticated user may exploit this vulnerability on Windows 2000/XP servers to execute arbitrary code with system-level privileges.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>NETBIOS:ACCESS:ADMIN</td>
<td>This signature detects attempts to exploit a null session vulnerability in NETBIOS SMB protocols. Attackers may initiate SMB sessions with no user name or password, obtain the remote admin share on the server, and use this information to plan further attacks.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>NETBIOS:ACCESS:C-DRIVE</td>
<td>This signature detects attempts to exploit a null session vulnerability in NETBIOS SMB protocols. Attackers may initiate SMB sessions with no user name or password, obtain the C Drive share on the server, and use this information to plan further attacks.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>NETBIOS:ACCESS:D-DRIVE</td>
<td>This signature detects attempts to exploit a null session vulnerability in NETBIOS SMB protocols. Attackers may initiate SMB sessions with no user name or password, obtain the D Drive share on the server, and use this information to plan further attacks.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>NETBIOS:NBDS:BAD_LABEL_FORMAT</td>
<td>This protocol anomaly is label for the second level encoding of a Netbios name that contains a pointer.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>NETBIOS:NBDS:INVALID:1STLVL_ENC</td>
<td>This protocol anomaly is an invalid first level encoding of a Netbios name.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>NETBIOS:NBDS:INVALID:DGM_LEN</td>
<td>This protocol anomaly is a Netbios datagram header with a DGM_LENGTH field value that is bigger than the packet length.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>NETBIOS:NBDS:INVALID:HDR_FLGS</td>
<td>This protocol anomaly is a Netbios datagram header with a FLAGS field that contains non-zero values for bits 0-3.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>NETBIOS:NBDS:INVALID:LABEL_LEN</td>
<td>This protocol anomaly is a label for the second level encoding of a netbios name; the label length is larger than 63, or the label is the first label and the length is not 32.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>NETBIOS:NBDS:INVALID:MSG_TYPE</td>
<td>This protocol anomaly is a Netbios datagram header with a MSG_TYPE field value that is invalid.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>NETBIOS:NBDS:INVALID:PROTO</td>
<td>This protocol anomaly is a Netbios message with a USER_DATA section that is less than the size of SMB header, or the protocol field of the SMB header does not start with 0xff 'S' 'M' 'B'.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>NETBIOS:NBDS:OVERFLOW:MSG</td>
<td>This protocol anomaly is a Netbios datagram that is bigger than 1064.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>NETBIOS:NBDS:OVERFLOW:NAME</td>
<td>This protocol anomaly is a Netbios name that is longer than 255.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>NETBIOS:NBNS:C2S_AA_FLAG</td>
<td>This protocol anomaly is query message with an NM_FLAGS field containing an authoritative answer flag that is set.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>NETBIOS:NBNS:C2S_RESPONSE</td>
<td>This protocol anomaly is query message with an OPCODE field containing an response flag that is set.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>NETBIOS:NBNS:CLASS-UNKNOWN</td>
<td>This protocol anomaly is an invalid value in the QUESTION_CLASS field of the question section or in the RR_CLASS field of the resource record header.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>NETBIOS:NBNS:INVALID:FIRST-ENC</td>
<td>This protocol anomaly is an invalid first level encoding of a Netbios name.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>NETBIOS:NBNS:INVALID:HDR-CNT</td>
<td>This protocol anomaly is a 1) a query message with ARCOUNT (answer count) or NSCOUNT (number of records in the authority section of a name service packet) fields of the header that are not zero, or 2) a response message with a QDCOUNT (number of entries in the question section) that is not zero.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>NETBIOS:NBNS:INVALID:HDR-OPCODE</td>
<td>This protocol anomaly is a header with an OPCODE field value that is not 0, 5, 6, 7, or 8.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>NETBIOS:NBNS:INVALID:HDR-Z</td>
<td>This protocol anomaly is a Netbios name header with a NM_FLAGS field that contains non-zero values for bit 4 or bit 5.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>NETBIOS:NBNS:INVALID:LABEL-LEN</td>
<td>This protocol anomaly is a label for the second level encoding of a Netbios name that has a label length larger than 63, or the label is the first label and the length is not 32.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>NETBIOS:NBNS:INVALID:NAME-FLGS</td>
<td>This protocol anomaly is a Netbios name header with a NM_FLAGS field that contains non-zero values for bits 3-15.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>NETBIOS:NBNS:INVALID:PTR</td>
<td>This protocol anomaly is a pointer offset in the second level encoding of a Netbios name that exceeds the message length (the pointer is pointing out of the message).</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>NETBIOS:NBNS:INVALID:RRNB-FLG</td>
<td>&quot;This protocol anomaly is a type node status response message&quot;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NETBIOS:NBNS:NAME_TOO_LONG</td>
<td>This protocol anomaly is a Netbios name that is longer than 255.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>NETBIOS:NBNS:POINTER_LOOP</td>
<td>This protocol anomaly is a second level encoding of a Netbios name that contains more nested pointers than the user-defined maximum. Default setting for the sc_nbname_pointer_loop_limit is 8.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>NETBIOS:NBNS:RESCODE:FORMAT_ERR</td>
<td>This protocol anomaly is Netbios name response with an RCODE that indicates the request has an invalid format.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>NETBIOS:NBNS:S2C_QUERY</td>
<td>This protocol anomaly is a Netbios name response header with an OPCODE field that contains an unset response bit.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>NETBIOS:NBNS:SHORT_MSG</td>
<td>This protocol anomaly is a Netbios name message that is shorter than expected.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>NETBIOS:NBNS:TYPE_UNKNOWN</td>
<td>This protocol anomaly is an invalid value in 1) the QUESTION_TYPE field in the question section or 2) the RR_TYPE field in the resource record header.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:AUDIT:GNUTELLA-BYE-TTL</td>
<td>This protocol anomaly is a Gnutella BYE message that does not contain a TTL of 1 and a HOPS of 0.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:AUDIT:GNUTELLA-EOL</td>
<td>This protocol anomaly is a Gnutella message that does not use the end-of-line (EOL) terminator characters \r\n.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:AUDIT:GNUTELLA-HDR-ATRB</td>
<td>This protocol anomaly is a Gnutella message with a header line that does not have a value for an attribute; a blank space exists after the attribute colon.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:AUDIT:GNUTELLA-HTTP-GET</td>
<td>This protocol anomaly is a Gnutella GET command that does not use the expected syntax. Correct syntax is: GET /get/&lt; File Index&gt;//&lt; File Name&gt; HTTP/1.1&lt; CR&gt;&lt; LF&gt;.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:AUDIT:GNUTELLA-LINE</td>
<td>This protocol anomaly is a Gnutella message with a line length that exceeds the user-defined maximum number of bytes. The default line length is 2048.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:AUDIT:GNUTELLA-MESSAGE</td>
<td>This protocol anomaly is a Gnutella message with a payload type that is not defined in the Gnutella RFC.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:AUDIT:GNUTELLA-MSG</td>
<td>This protocol anomaly is a Gnutella message with a payload length that exceeds 4096 bytes.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:AUDIT:GNUTELLA-OK-RESP</td>
<td>This protocol anomaly is a Gnutella client response that does not use the expected syntax. Correct syntax for Gnutella 0.6 is: GNUTELLA/0.6 200 OK&lt; CR&gt;&lt; LF&gt;.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:AUDIT:GNUTELLA-PING-LEN</td>
<td>This protocol anomaly is a Gnutella 0.4 PING message that has a non-zero payload length.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:AUDIT:GNUTELLA-PONG-LEN</td>
<td>This protocol anomaly is a Gnutella PONG message that has an invalid payload length. Gnutella 0.4 PONG messages should have exactly 14 bytes; Gnutella 0.6 PONG messages should have a minimum of 14 bytes.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:AUDIT:GNUTELLA-PUSH-LEN</td>
<td>This protocol anomaly is a Gnutella PUSH message with a payload length that is less than 26 bytes.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:AUDIT:GNUTELLA-QUERY</td>
<td>This protocol anomaly is a Gnutella QUERY message with a payload length that exceeds the user-defined maximum number of bytes. The default line length is 256.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>P2P:AUDIT:GNUTELLA-RTABLE-UPD</td>
<td>This protocol anomaly is a Gnutella ROUTE_TABLE_UPDATE message with a payload length of 0 bytes.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:AUDIT:GNUTELLA-SEARCH</td>
<td>This protocol anomaly is a Gnutella message with a search criteria field that does not end with a NULL character.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:AUDIT:GNUTELLA-SVR-RESP</td>
<td>This protocol anomaly is a Gnutella server response that does not use the expected syntax. Correct syntax for Gnutella 0.4 is: GNUTELLA OK&lt;CR&gt;&lt;LF&gt;; correct syntax for Gnutella 0.6 is: GNUTELLA/0.6 200 OK&lt;CR&gt;&lt;LF&gt;.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:AUDIT:GNUTELLA-TTL</td>
<td>This protocol anomaly is a Gnutella message with a TTL that exceeds the user-defined maximum. The default TTL is 8. The Gnutella RFC recommends an 8 to 10 TTL maximum for Gnutella messages.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:AUDIT:GNUTELLA-UNSUP-VER</td>
<td>This protocol anomaly is a Gnutella message with a connect string that does not conform to Gnutella RFC or the requesting Gnutella version is not 0.4 or 0.6.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:BITTORRENT:TRACKER-QUERY</td>
<td>This signature detects requests to a BitTorrent tracker website. Users may be querying the tracker to look for files to download.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:BITTORRENT:TRACKER-SCRAPE</td>
<td>This signature detects 'scrape' requests to a BitTorrent tracker website. Users may be querying the tracker to look for files to download.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:DC:DC-PP-ACTIVE</td>
<td>This signature detects use of the Direct Connect Plus Plus (DC++) file sharing client.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:EDONKEY:CLIENT-VER-CHECK</td>
<td>This signature detects version checks by eDonkey 2000, a peer-to-peer file sharing client. The eDonkey client occasionally checks its own version number to ensure that the client is current.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:GNUTELLA:CONNECT</td>
<td>This signature detects Gnutella client connection requests. Because Gnutella does not use a fixed port number, this signature searches TCP connections to port 1024 and higher by default.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:GNUTELLA:CONNECTION-OK</td>
<td>This signature detects Gnutella server responses to a connection request. Because Gnutella does not use a fixed port number, this signature searches TCP connections to port 1024 and higher by default.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:GNUTELLA:CONNECTION-OK-V06</td>
<td>This signature detects Gnutella server responses to a connection request. Because Gnutella does not use a fixed port number, this signature searches TCP connections to port 1024 and higher by default.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:MLDONKEY:CLIENT-ACTIVE</td>
<td>This signature detects activity by the peer-to-peer (P2P) file sharing client MLDonkey, a multi-protocol P2P file sharing application.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:SKYPE:VERSION-CHECK</td>
<td>This signature detects a Skype client request (to a central server) that checks for the latest version of the client software.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:WINMX:CLIENT-MATCHMAKE-DNS</td>
<td>This signature detects a WinMX client performing DNS lookups for matchmaking servers. WinMX is a peer-to-peer file sharing client that tests firewall rules and reverse-connectivity to determine the most effective way to share files. WinMX queries a matchmaking server to obtain Supernode lists, which enable the WinMX client to share files.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>--------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>P2P:WINMX:CLIENT-NET-PRB-DNS</td>
<td>This signature detects a WinMX client performing DNS lookups for hosts that WinMX will probe for connectivity. WinMX is a peer-to-peer file sharing client that tests firewall rules and reverse-connectivity to determine the most effective way to share files.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:WINMX:CLIENT-VER-ChK</td>
<td>This signature detects an initial connection by WinMX, a peer-to-peer file sharing client. WinMX queries a Web site for new versions of the WinMX client software.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:WINMX:CLIENT-VER-ChK-DNS</td>
<td>This signature detects attempts to obtain the IP address of the host that tracks WinMX client versions. WinMX is a peer-to-peer file sharing client.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:DOS:MDAEMON-POP-DOS</td>
<td>This signature detects denial-of-service attempts against the Mdaemon POP3 Server. Mdaemon v.6.0.7 and earlier versions are vulnerable. Attackers may send a maliciously crafted DELE or UIDL request to the POP3 daemon to crash the POP3, SMTP, and IMAP services.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>POP3:ERROR:BOUNDARY_MISSING</td>
<td>This protocol anomaly is a message with a multipart content type but no boundary.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-386</td>
<td>This signature detects email attachments that have the extension .386 and were received via POP3. Because .386s (Windows Enhanced Mode Driver) files contain executable code, this may indicate an incoming email virus. Attackers may create malicious executables, tricking users into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-ADE</td>
<td>This signature detects email attachments that have the extension .ade and were received via POP3. Because .ADEs (Microsoft Access Project Extension) files contain macros, this may indicate an incoming email virus. Attackers may create malicious scripts, tricking users into executing the macros and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-ADP</td>
<td>This signature detects email attachments that have the extension .adp and were received via POP3. Because .ADPs (Microsoft Access Project) files can contain macros, this may indicate an incoming email virus. Attackers may create malicious scripts, tricking users into executing the macros and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-BAS</td>
<td>This signature detects email attachments that have the extension .bas and were received via POP3. Because .BASs (Microsoft Visual Basic Class Module) files contain executable code, this may indicate an incoming email virus. Attackers may create malicious executables, tricking users into executing the file and infecting the system.</td>
<td>low</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-BAT</td>
<td>This signature detects email attachments with the extension .bat received via POP3. This may indicate an incoming email virus. .BATS (executable files) contain one or more scripts. Attackers may create malicious executables, tricking the user into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-CHM</td>
<td>This signature detects email attachments that have the extension .chm and were received via POP3. Because .CHMs (Compiled HTML Help File) files can contain scripts, this may indicate an incoming email virus. Attackers may create malicious scripts, tricking users into executing the files and infecting the system.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>POP3:EXT:DOT-CMD</td>
<td>This signature detects email attachments with the extension &quot;.cmd&quot; sent via POP3. This may indicate an incoming email virus. CMD files contain commands that when executed can cause significant damage to a windows system.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-COM</td>
<td>This signature detects email attachments with the extension &quot;.com&quot; received via POP3. This may indicate an incoming email virus. COMs (executable files) contain one or more scripts. Attackers may create malicious executables, tricking the user into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-CPL</td>
<td>This signature detects email attachments with the extension &quot;.cpl&quot; received via POP3. This may indicate an incoming email virus. CPLs (Control Panel eLements) are standard Microsoft Windows files that contain Windows Control Panel settings. Attackers may hide malicious executables within a CPL file, tricking users into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-CRT</td>
<td>This signature detects email attachments that have the extension .crt and were received via POP3. Because .CRTs (Security Certificate) files can contain executable code, this may indicate an incoming email virus. Attackers may create malicious executable code, tricking users into executing the file and infecting the system.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-EXE</td>
<td>This signature detects email attachments with the extension &quot;.exe&quot; sent via POP3. This may indicate an incoming email virus. EXEs (Executable files) contain one or more scripts. Attackers may create malicious executables, tricking the user into executing the file and infecting the system.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-GRP</td>
<td>This signature detects GRP files sent over POP3. GRP files can contain Windows Program Group information, and may be exploited by malicious users to deposit instructions or arbitrary code on a target's system. User involvement is required to activate GRP files; typically they are attached to a harmless-appearing e-mail message.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-HLP</td>
<td>This signature detects email attachments that have the extension .hlp and were received via POP3. Because .HLPs (Help File) files can contain macros, this may indicate an incoming email virus. Attackers may create malicious scripts, tricking users into executing the macros and infecting the system.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-HT</td>
<td>This signature detects email attachments with the extension &quot;.ht&quot; sent via POP3. This may indicate an incoming email virus or other attack. HT files contain configuration information for the Hyperterm console program, shipped with every Windows operating system since Windows 95. It is the default handler program for .ht files. A recent vulnerability in Hyperterm could allow an attacker to take control of your computer via an infected .ht file. These files are not normally sent via email.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-HTA</td>
<td>This signature detects email attachments with the extension .hta received using POP3. This may indicate an incoming email virus. HTA files are HTML application files that can be executed by a web browser. Generally, HTA files are not sent via email. As a general network security precaution, ensure that all users are aware of the dangers of sending and receiving binary files in email attachments.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>POP3:EXT:DOT-INF</td>
<td>This signature detects email attachments that have the extension .inf and were received via POP3. Because .INFs (Setup Information) files contain scripts, this may indicate an incoming email virus. Attackers may create malicious scripts, tricking users into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-INS</td>
<td>This signature detects email attachments that have the extension .ins and were received via POP3. Because .INSs (Internet Naming Service) files contain configuration parameters, this may indicate an incoming email virus. Attackers may include malicious configurations, tricking users into executing the file and infecting the system.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-ISP</td>
<td>This signature detects email attachments that have the extension .isp and were received via POP3. Because .ISPs (Internet Communication Settings) files contain configuration parameters, this may indicate an incoming email virus. Attackers may include malicious configurations, tricking users into executing the file and infecting the system.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-JS</td>
<td>This signature detects email attachments that have the extension .ss and were received via POP3. Because .JSS (JavaScript File) files contain scripts, this may indicate an incoming email virus. Attackers may create malicious scripts, tricking users into executing the file and infecting the system.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-JSE</td>
<td>This signature detects email attachments that have the extension .jse and were received via POP3. Because .JSEs (JavaScript Encoded) files contain scripts, this may indicate an incoming email virus. Attackers may create malicious scripts, tricking users into executing the file and infecting the system.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-LNK</td>
<td>This signature detects email attachments that have the extension .lnk and were received via POP3. Because .LNKs (Windows link) files can point to any program, this may indicate an incoming email virus. Attackers may create a link pointing to a dangerous program, tricking users into executing the link and affecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-MDB</td>
<td>This signature detects email attachments that have the extension .mdb and were received via POP3. Because .MDBs (MS Access Application) files can contain scripts, this may indicate an incoming email virus. Attackers may create malicious scripts, tricking users into executing the file and infecting the system.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-MDE</td>
<td>This signature detects email attachments that have the extension .mde and were received via POP3. Because .MDEs (Microsoft Access MDE database) files can contain scripts and macros, this may indicate an incoming email virus. Attackers may create malicious scripts, tricking users into executing the file and infecting the system.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-MSC</td>
<td>This signature detects email attachments that have the extension .msc and were received via POP3.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>POP3:EXT:DOT-MSI</td>
<td>This signature detects email attachments with the extension <code>.msi</code> received via POP3. This may indicate an incoming email virus. .MSIs (Microsoft Windows Installer Package) contain executable code. Attackers may create malicious executables, tricking the user into executing the file and infecting the system.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-MSP</td>
<td>This signature detects email attachments with the extension <code>.msp</code> received via POP3. This may indicate an incoming email virus. .MSPs (Microsoft Windows Installer Patch) contain executable code. Attackers may create malicious executables, tricking the user into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-OCX</td>
<td>This signature detects email attachments that have the extension <code>.ocx</code> and were received via POP3. Because .OCXs (Object Control Extension) files can contain multiple scripts, this may indicate an incoming email virus. Attackers may create malicious executables, tricking users into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-PCD</td>
<td>This signature detects email attachments that have the extension <code>.pcd</code> and were received via POP3. Because .PCDs (Photo CD MS Compiled Script) files contain scripts, this may indicate an incoming email virus. Attackers may create malicious scripts, tricking users into executing the file and infecting the system.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-PIF</td>
<td>This signature detects email attachments with the extension <code>.pif</code> sent via POP3. This may indicate an incoming email virus. PIFs (Program Information Files) are standard Microsoft Windows files that contain start up properties for DOS applications. Attackers may hide malicious executables within a PIF file, tricking users into executing the file and infecting the system.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-REG</td>
<td>This signature detects email attachments that have the extension <code>.reg</code> and were received via POP3. Because .REGs (Registry Entries) files contain entries for the Registry, this may indicate an incoming email virus. Attackers may create malicious entries, tricking users into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-SCR</td>
<td>This signature detects email attachments with the extension <code>.scr</code> sent via POP3. This may indicate an incoming email virus. SCRs (ScreenSaver files) are renamed <code>.exe</code> files containing executable code. Attackers may disguise malicious executables to appear as harmless screensaver files, tricking the user into executing the file and infecting the system.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-SCT</td>
<td>This signature detects email attachments with the extension <code>.sct</code> received via POP3. This may indicate an incoming email virus. .SCTs (Windows Script Component) contain scripts. Attackers may create malicious scripts, tricking the user into executing the file and infecting the system.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-URL</td>
<td>This signature detects email attachments with the extension <code>.url</code> received via POP3. This may indicate an incoming email virus. .URLs (Internet Shortcut) contain a link to a web location. Attackers may create a malicious shortcut, tricking the user into executing the file and send the user to a malicious website.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>POP3:EXT:DOT-VB</td>
<td>This signature detects email attachments with the extension .vb received via POP3. This may indicate an incoming email virus. VBs (VBScript File) contain scripts. Attackers may create malicious scripts, tricking the user into executing the file and infecting the system.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-VBE</td>
<td>This signature detects email attachments with the extension .vbe received via POP3. This may indicate an incoming email virus. VBEs (VBScript Encoded Script File) contain scripts. Attackers may create malicious scripts, tricking the user into executing the file and infecting the system.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-VBS</td>
<td>This signature detects email attachments with the extension .vbs sent via POP3. This may indicate an incoming email virus. VBSs (Visual Basic files) contain one or more executable scripts. Attackers may create malicious VB files, tricking the user into executing the file and infecting the system.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-WMF</td>
<td>This signature detects Metafiles files sent over POP. Windows Metafiles and Enhanced Metafiles files can exploit a Windows GDI vulnerability and may be exploited by malicious users to deposit instructions or arbitrary code on a target's system. User involvement is required to activate Metafiles; typically they are attached to a harmless-appearing e-mail message.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-WSC</td>
<td>This signature detects email attachments with the extension .wsc received via POP3. This may indicate an incoming email virus. WSCs (Windows Script Component) contain scripts. Attackers may create malicious scripts, tricking the user into executing the file and infecting the system.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-WSF</td>
<td>This signature detects email attachments with the extension .wsf received via POP3. This may indicate an incoming email virus. WSFs (Windows Script File) contain scripts. Attackers may create malicious scripts, tricking the user into executing the file and infecting the system.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-WSH</td>
<td>This signature detects email attachments with the extension .wsh received via POP3. This may indicate an incoming email virus. WSHs (Windows Script Host Settings File) contain configuration parameters. Attackers may create malicious configurations, tricking the user into executing the file and infecting the system.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-ZIP</td>
<td>This signature detects email attachments with the extension .zip received using POP3. This may indicate an incoming email virus. Zip files are compressed files that can contain one or more executables. Attackers may compress malicious executables within a .zip file, tricking unsuspecting users into executing the file and infecting the system. Because Zip files are frequently used for non-malicious purposes, this signature can generate false positives. As a general network security precaution, ensure that all users are aware of the dangers of sending and receiving binary files in email attachments.</td>
<td>low</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOUBLE-DOT-DOT</td>
<td>This signature detects email attachments that contain two file extensions. Attackers or viruses may send email attachments that use two file extensions to disguise the actual file name and trick users into opening a malicious attachment.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>POP3:FAILURE:BRUTE-FORCE</td>
<td>This protocol anomaly is multiple login failures within a short period of time between a unique pair of hosts. The default is 4.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:OUTLOOK:TROUBLE-QUERY-OF</td>
<td>This signature detects buffer overflow attempts against an ActiveX control in Microsoft Outlook. The Local Troubleshooter ActiveX control has inadequate bounds for checking for its Query function, and this exploit bypasses normal Outlook/IE ActiveX security controls. Attackers may create a malicious Web site that contains a call to this ActiveX control; this call contains an overly long string that overflows the control buffer, enabling the attacker to gain control of the target system with the user privileges.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:OVERFLOW:APOP</td>
<td>This protocol anomaly is a POP3 APOP command argument that is too long. This may indicate a buffer overflow attempt.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>POP3:OVERFLOW:BOUNDARY_OVERFLOW</td>
<td>This protocol anomaly is a message with more than 70 boundary characters.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:OVERFLOW:COMMAND</td>
<td>This protocol anomaly is a POP3 command that exceeds 4 bytes, the standard length for a POP3 command. This may indicate a non-standard POP3 client/server or an attacker has gained command-line access to the server.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>POP3:OVERFLOW:CONTENT_NAME</td>
<td>This protocol anomaly is a mime header content-type with a name length that is longer than the defined value. The default value is 128.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:OVERFLOW:FILENAME2LONG</td>
<td>This protocol anomaly is a message with a content_disposition header containing a 'name' attribute value that is too long.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:OVERFLOW:LINE</td>
<td>This protocol anomaly is a text-line from a POP3 client to the server that is too long. This may indicate a buffer overflow attempt.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>POP3:OVERFLOW:PASS</td>
<td>This protocol anomaly is a POP3 PASS command argument that is too long. This may indicate a buffer overflow attempt.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>POP3:OVERFLOW:QPOP-OF1</td>
<td>This signature detects buffer overflow attempts against Qpopper, a POP3 server for Unix. Qpopper 3.0beta20 and earlier versions are vulnerable.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>POP3:OVERFLOW:QPOP-OF2</td>
<td>This signature detects a buffer overflow attempt to exploit a vulnerability in Qpopper. Version 3.0beta30 and many earlier versions are vulnerable.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>POP3:OVERFLOW:QPOP-OF3</td>
<td>This signature detects buffer overflow attempts to exploit a vulnerability in the Qpopper daemon. Some 3.0 beta versions are vulnerable.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>POP3:OVERFLOW:QPOP-OF4</td>
<td>This signature detects a buffer overflow attempt to exploit a vulnerability in Qpopper using custom shellcode. Version 3.0beta20 and many earlier versions are vulnerable.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>POP3:OVERFLOW:TEXTLINE_2LONG</td>
<td>This protocol anomaly is a message data line that exceeds the defined maximum length (sc_mime_textline_length).</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:OVERFLOW:USER</td>
<td>This protocol anomaly is a POP3 USER command argument that is too long. This may indicate a buffer overflow attempt.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-------------</td>
<td>--------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>POP3:REQERR:REQ-MESSAGE-NUMBER</td>
<td>This protocol anomaly is a POP3 message number that is unreasonably high. This may indicate a huge mailbox or an exploit attempt.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>POP3:REQERR:REQ-SYNTAX-ERROR</td>
<td>This protocol anomaly is an unparsed POP command line or header line. This may indicate a non-standard email client or server or a backdoor/exploit attempt.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>SCAN:AMAP:FTP-ON-HTTP</td>
<td>This signature detects the scanner tool amap, made by The Hacker’s Choice. THC-AMAP is used in initial reconnaissance for an attacker to determine services running on target hosts before launching other attacks.</td>
<td>low</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SCAN:AMAP:SAP-R3-ON-HTTP</td>
<td>This signature detects the scanner tool AMAP, made by The Hacker’s Choice (THC). Attackers may use THC-AMAP during their initial reconnaissance to determine services running on target hosts before launching other attacks.</td>
<td>low</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SCAN:AMAP:SSL-ON-HTTP</td>
<td>This signature detects the scanner tool AMAP, made by The Hacker’s Choice (THC). Attackers may use THC-AMAP during their initial reconnaissance to determine services running on target hosts before launching other attacks.</td>
<td>low</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SCAN:AMAP:SSL-ON-POP3</td>
<td>This signature detects the scanner tool AMAP, made by The Hacker’s Choice (THC). Attackers may use THC-AMAP during their initial reconnaissance to determine services running on target hosts before launching other attacks.</td>
<td>low</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SCAN:METASPLOIT:SMB-ACTIVE</td>
<td>This signature detects traffic generated by the open-source exploiting tool Metasploit Framework. Other signatures may also trip. This indicates that someone is using this tool on your network. Follow-up investigation of source or target machines may be required.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SCAN:MISC:HTTP:HTR-OVERFLOW</td>
<td>“This signature detects denial-of-service (DoS) attacks against Microsoft IIS 4.0 and 5.0. Attackers may send maliciously crafted HTR requests (.htr) with long variable names to overflow the buffer in the ism.dll ISAPI extension that implements HTR scripting and create a denial of service or execute arbitrary commands.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>SHELLCODE:AIX:NOOP-PKT</td>
<td>This signature scans PACKETS for at least four in a raw AIX NOOP instructions, which are very common in buffer overflow exploits. You may want to apply this signature to all non-TCP traffic to your AIX servers.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>SHELLCODE:BSDX86:GEN-1-PKT</td>
<td>This signature scans PACKETS for an x86 BSD (all flavors) instruction sequence, common in buffer overflow exploits. You may want to apply this signature to all non-TCP traffic to your BSD servers.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>SHELLCODE:BSDX86:GEN-2-PKT</td>
<td>This signature scans PACKETS for an x86 BSD (all flavors) instruction sequence, common in buffer overflow exploits. You may want to apply this signature to all non-TCP traffic to your BSD servers.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>SHELLCODE:DIGITAL:NOOP-PKT</td>
<td>This signature scans PACKETS for at least four in a raw DEC ALPHA NOOP instructions, which are very common in buffer overflow exploits. You may want to apply this signature to all non-TCP traffic to your DEC ALPHA servers.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>SHELLCODE:HP-UX:HP-NOOP-1-PKT</td>
<td>This signature scans PACKETS for a HP-UX PA-RISC instruction sequence, common in buffer overflow exploits. You may want to apply this signature to all non-TCP traffic to your HP-UX servers.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>SHELLCODE:HP-UX:HP-NOOP-2-PKT</td>
<td>This signature scans PACKETS for a HP-UX PA-RISC instruction sequence, common in buffer overflow exploits. You may want to apply this signature to all non-TCP traffic to your HP-UX servers.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>SMB:AUDIT:INV-PROTOCOL</td>
<td>This protocol anomaly is an invalid SMB protocol. The first four bytes of valid SMB messages are 0xff, 'S', 'M', 'B'. This may be a misbehaving client or an attempt to tunnel through the NETBIOS port.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMB:CONNECT-FROM-LOCALHOST</td>
<td>This signature detects attempts to remotely connect to SMB shares with the NetBIOS hostname of Localhost. Because Localhost logins are not typically performed over the network, this may indicate that an attacker is trying to bypass host-based access controls.</td>
<td>low</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMB:ENUM:NAME-LOOKUP</td>
<td>This protocol anomaly is the \pipe\lsarpc (Local Security Authority) named pipe transaction used to execute the LookupAccountName function. Programs such as user2sid and Hyena use this named pipe transaction to validate usernames on the target host.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMB:ERROR:GRIND</td>
<td>This protocol anomaly is multiple login/authentication failures between a unique pair of hosts within a short period of time. Vulnerability scanners and programs like enum that perform dictionary based or password-guessing attacks will likely trigger this attack.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMB:ERROR:INV-MSG-LEN</td>
<td>This protocol anomaly is an invalid session message length in an SMB message.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMB:ERROR:MAL-MSG</td>
<td>This protocol anomaly is a malformed SMB message in which the wcount field is larger than the message size.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMB:EXPLOIT:ACCOUNT-NAME-OF</td>
<td>This signature detects attempts to overflow the SMB Account Name. ISS BlackICE, Proventia, and RealSecure products are vulnerable to this buffer overflow. A successful attack could give an attacker complete control of these systems.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMB:EXPLOIT:DOT-JOB</td>
<td>This signature detects a Microsoft Task Scheduler (.job) file being copied over an SMB network share. Microsoft Windows XP Service Pack 1 and Microsoft Windows 2000 Service Pack 2 and earlier are vulnerable. Attackers may open a malicious .job file in Task Scheduler to execute arbitrary code and compromise the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMB:EXPLOIT:LANMAN-NUKE</td>
<td>This protocol anomaly is a LANMAN request (NetServerEnum, NetServerEnum2, or NetShareEnum) over a named pipe transaction where the max-param-count and/or the max-data-count of the Transaction header is zero. Attackers can use this malformed request to crash an unpatched Microsoft NT, 2000, or XP server.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMB:EXPLOIT:LINUX-TRANS2-OF</td>
<td>This signature detects attempts to exploit a vulnerability in the Server Message Block File System (SMBFS) implemented in the Linux kernel. Kernels 2.4 and 2.6 are vulnerable. Attackers may gain root access on the target host.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMB:EXPLOIT:NULL-FIENAME</td>
<td>This protocol anomaly is an empty Filename field in the Delete, Rename, Move or Copy SMBs.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMB:EXPLOIT:NULL-PATH</td>
<td>This protocol anomaly is an empty Path field in the Tree Connect SMB. This may be a misbehaving client or an attempt to exploit vulnerabilities in the SMB server.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>--------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>SMB:EXPLOIT:NULL-SERVICE</td>
<td>This protocol anomaly is an empty Service field in the Tree</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td></td>
<td>Connect SMB. This may be a misbehaving client or an attempt</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>to exploit vulnerabilities in the SMB server.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMB:EXPLOIT:REGISTRY-DOS</td>
<td>DI has detected a suspiciously large registry key in the</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td></td>
<td>OpenKey function executed using a named-pipe transaction.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Large key sizes in the OpenKey function can cause the</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>winlogon.exe process in Windows NT 4.0 to crash.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMB:EXPLOIT:SAMBA-DIR-TRAV</td>
<td>This signature detects SMB requests for pathnames that attempt</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td></td>
<td>to traverse the server root. Samba 3.0.5 and earlier versions</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>are vulnerable. Malicious users can send &quot;get&quot;, &quot;put&quot;, and</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>&quot;dir&quot; commands to a Samba server to access files outside the</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>shared directories.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMB:EXPLOIT:WINBLAST-DOS</td>
<td>Microsoft Windows Samba File Sharing Resource Exhaustion</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td></td>
<td>Vulnerability</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMB:NETBIOS:INV-CDNAME-ENC</td>
<td>This protocol anomaly is an invalid calling name encoding</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td></td>
<td>in the NETBIOS header that encapsulates an SMB. NETBIOS</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>names are 16 bytes and may encode to a maximum of 34 bytes.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMB:NETBIOS:INV-CDNAME-LEN</td>
<td>This protocol anomaly is an invalid called name length in</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td></td>
<td>the NETBIOS header that encapsulates an SMB. NETBIOS names</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>are 16 bytes and may encode to a maximum of 34 bytes.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMB:NETBIOS:INV-CGNAME-ENC</td>
<td>This protocol anomaly is an invalid calling name encoding</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td></td>
<td>in the NETBIOS header that encapsulates an SMB. NETBIOS</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>names are 16 bytes and may encode to a maximum of 34 bytes.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMB:NETBIOS:INV-CGNAME-LEN</td>
<td>This protocol anomaly is an invalid called name length in</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td></td>
<td>the NETBIOS header that encapsulates an SMB. NETBIOS names</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>are 16 bytes and may encode to a maximum of 34 bytes.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMB:NETBIOS:INV-SHDR-LEN</td>
<td>This protocol anomaly is an invalid session header length in</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td></td>
<td>the NETBIOS header that encapsulates an SMB. The minimum</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>length of an SMB message is 33 bytes.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMB:NETBIOS:INV-SNAME-LEN</td>
<td>This protocol anomaly is an invalid session name length in</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td></td>
<td>the NETBIOS header that encapsulates an SMB. NETBIOS names</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>are 16 bytes and may encode to a maximum of 34 bytes.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMB:NETBIOS:RMT-REG-ACCESS</td>
<td>This signature detects attempts to remotely access the</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td></td>
<td>Windows registry. Attackers may use a malicious client to</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>view or modify the contents of the Windows registry.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMB:NETBIOS:SHARE-LVL-SEC</td>
<td>This protocol anomaly is an SMB session with share-level</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td></td>
<td>security. A user may gain access to various resources on the</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>server without username or password authentication.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMB:TOOLS:PSEEXEC</td>
<td>This signature detects attempts to upload psexec.exe, an</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td></td>
<td>SMB tool for uploading and executing programs interactively.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>This signature also indicates that the psexec.exe has</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>already logged into the system; Psexec.exe can upload itself</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>to the host only after successful login. Worms often use</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>psexec.exe to propagate.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMTP:AUDIT:REQ-INVALID-CMD-SEQ</td>
<td>This protocol anomaly is an invalid sequence of SMTP</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td></td>
<td>commands, which would normally not be issued by an SMTP</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>client or server. This may indicate an attacker manually</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>trying to exploit an SMTP server.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>SMTP:AUDIT:TEXT-LINE</td>
<td>This protocol anomaly is a text line (in the data section) in an SMTP connection that is too long. This may indicate a buffer overflow attempt.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:COMMAND:EXPN</td>
<td>This protocol anomaly is an attempt to use the EXPN command. This command is not used by most standard clients and servers and may reveal information about email accounts.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>SMTP:COMMAND:TURN</td>
<td>This protocol anomaly is an attempt to use the TURN command that exchanges the roles of the email client and server. You may want to ban this command and drop the connection, or edit the SMTP attack objects and change their direction to `BOTH. `</td>
<td>`medium`</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:COMMAND:VRFY</td>
<td>This protocol anomaly is an attempt to use the SMTP VRFY command. This command is not used by most standard clients and servers and may reveal sensitive information about email accounts.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>SMTP:COMMAND:WIZ</td>
<td>This signature detects attempts to determine if the SMTP server supports the `WIZ` command, which may provide anonymous root access.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EMAIL:EUDORA-SPOOF3</td>
<td>This signature detects attempts to spoof an email attachment. Eudora Windows versions prior to up to 6.0.3 are vulnerable. Attackers may send a maliciously crafted email with an illegal &quot;Attachment Converted:&quot; line in the message body to spoof attachments, which can lead to remote code execution.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EMAIL:EUDORA-SPOOF4</td>
<td>This signature detects attempts to spoof an email attachment. Eudora Windows 6.2.0.7 and earlier versions are vulnerable. Attackers may send a maliciously crafted email with an illegal &quot;Attachment Converted:&quot; line in the message body to spoof attachments, which can enable remote code execution.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EMAIL:HEADER-FROM-PIPE</td>
<td>This signature detects attempts to send shell commands via an SMTP email message by exploiting the pipe passthrough vulnerability. Attackers may use the invalid &quot;from</td>
<td>as the return email address to cause Sendmail to reroute data to another program.</td>
<td>medium</td>
</tr>
<tr>
<td>SMTP:EMAIL:HEADER-TO-PIPE</td>
<td>This signature detects attempts to send shell commands via an SMTP email message by exploiting the pipe passthrough vulnerability. Attackers may use the invalid &quot;to</td>
<td>as the return email address to cause Sendmail to reroute data to another program.</td>
<td>medium</td>
</tr>
<tr>
<td>SMTP:EMAIL:MAIL-FROM-PIPE</td>
<td>This signature detects attempts to send shell commands via an SMTP email message by exploiting the pipe passthrough vulnerability. Attackers may use the invalid &quot;mail from</td>
<td>as the return email address to cause Sendmail to reroute data to another program.</td>
<td>medium</td>
</tr>
<tr>
<td>SMTP:EMAIL:RCPT-TO-DECODE</td>
<td>This signature detects attempts to send shell commands via an SMTP email message by exploiting the &quot;decode&quot; email alias vulnerability. Attackers may use the invalid &quot;rcpt to decode&quot; as the &quot;rcpt to</td>
<td>email address to cause Sendmail to reroute data to the program uudecode. Attackers may then send uuencoded data to overwrite files or place an arbitrary .rhosts files onto the system.</td>
<td>high</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>SMTP:EMAIL:RCPT-TO-PIPE</td>
<td>This signature detects attempts to send shell commands via an SMTP email message by exploiting the pipe passthrough vulnerability. Attackers may use the invalid &quot;rcpt to</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td></td>
<td>&quot; as the &quot;rcpt to&quot; email address to cause Sendmail to reroute data to another program. Some SMTP servers have been shown to use the &quot; character legitimately.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMTP:EMAIL:REPLY-TO-PIPE</td>
<td>This signature detects attempts to send shell commands via an SMTP email message by exploiting the pipe passthrough vulnerability. Attackers may use the invalid &quot;reply to</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td></td>
<td>&quot; as the &quot;reply to&quot; email address to cause Sendmail to reroute data to another program. This may also be legitimate traffic from several types of SMTP servers.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMTP:EXCHANGE:DOS</td>
<td>This signature detects denial-of-service (DoS) attempts that exploit a MIME header vulnerability in Microsoft Exchange Server 5.5. Attackers may send an email message with an empty charset value (&quot;&quot;&quot;) in the MIME header to cause a denial-of-service (DoS).</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXCHANGE:INV_BDAT_CMD</td>
<td>This protocol anomaly is a BDAT command that is not chunk-size.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXCHANGE:INV_BDAT_SEC_LEN</td>
<td>This protocol anomaly is a BDAT with a chunk-size larger than 0xffffffff.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXCHANGE:MAL-VERB-XEXCH50</td>
<td>This signature detects attempts to exploit a vulnerability in Microsoft Exchange Server 5.5 and 2000. The command verb &quot;Xexch50&quot;, which is valid only for communication between validated Exchange servers, is handled incorrectly. Attackers may send the command verb with a negative number or a very large positive number to crash the Exchange server, and, in extreme cases with Exchange Server 2000, may also take control of the server.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXPLOIT:EUDORA-URL-SPOOF</td>
<td>This signature detects attempts to exploit a vulnerability in the Eudora mail client. By supplying a link containing character entities, an attacker can force Eudora to display a link as something other than what it really is.</td>
<td>low</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXPLOIT:HCP-QUOTE-SCRIPT</td>
<td>This signature detects attempts to exploit a vulnerability in URL handling with the Microsoft Help and Support Center (HSC) when invoked with an hcp:// URL. By embedding a quote (&quot;&quot;&quot;) character in the URL, HSC can be instructed to load an arbitrary local file or remote web page, which can then be used to execute scripts in the local zone.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXPLOIT:MIME-TOOLS-EVADE</td>
<td>This signature detects attempts to evade antivirus tools such as MIME Tools, a Linux-based email MIME scanner. The MIME RFC allows for an empty boundary, but most all mail clients use one, while many viruses will not.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-386</td>
<td>This signature detects email attachments that have the extension .386 and were sent via SMTP. Because .386s (Windows Enhanced Mode Driver) files can contain executable code, this may indicate an incoming email virus. Attackers may create malicious executables, tricking users into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-ADE</td>
<td>This signature detects email attachments that have the extension .ade and were sent via SMTP. Because .ADEs (Microsoft Access Project Extension) files can contain macros, this may indicate an incoming email virus. Attackers may create malicious scripts, tricking users into executing the macros and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-ADP</td>
<td>This signature detects email attachments that have the extension .adp and were sent via SMTP. Because .ADPs (Microsoft Access Project) files can contain macros, this may indicate an incoming email virus. Attackers may create malicious scripts, tricking users into executing the macros and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-BAS</td>
<td>This signature detects email attachments that have the extension .bas and were sent via SMTP. Because .BASs (Microsoft Visual Basic Class Module) files contain executable code, this may indicate an incoming email virus. Attackers may create malicious executables, tricking users into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-BAT</td>
<td>This signature detects email attachments with the extension '.bat' sent via SMTP. This may indicate an incoming email virus. .BATs (executable files) contain one or more scripts. Attackers may create malicious executables, tricking the user into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-CHM</td>
<td>This signature detects email attachments that have the extension .chm and were sent via SMTP. Because .CHMs (Compiled HTML Help File) files can contain scripts, this may indicate an incoming email virus. Attackers may create malicious scripts, tricking users into executing the files and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-CMD</td>
<td>This signature detects email attachments with the extension '.cmd' sent via SMTP. This may indicate an incoming email virus. CMD files contain commands that when executed can cause significant damage to a windows system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-COM</td>
<td>This signature detects email attachments with the extension '.com' sent via SMTP. This may indicate an incoming email virus. .COMs (executable files) contain one or more scripts. Attackers may create malicious executables, tricking the user into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-CPL</td>
<td>This signature detects email attachments with the extension '.cpl' sent via SMTP. This may indicate an incoming email virus. CPLs (Control Panel eLements) are standard Microsoft Windows files that contain Windows Control Panel settings. Attackers may hide malicious executables within a CPL file, tricking users into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-CRT</td>
<td>This signature detects email attachments that have the extension .crt and sent received via SMTP. Because .CRTs (Security Certificate) files can contain executable code, this may indicate an incoming email virus. Attackers may create malicious executable code, tricking users into executing the file and infecting the system.</td>
<td>low</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-EXE</td>
<td>This signature detects email attachments with the extension '.exe' sent via SMTP. This may indicate an incoming email virus. .EXEs (executable files) contain one or more scripts. Attackers may create malicious executables, tricking the user into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
</tbody>
</table>
## SMTP:EXT:DOT-GRP
This signature detects GRP files sent over SMTP. GRP files can contain Windows Program Group information, and may be exploited by malicious users to deposit instructions or arbitrary code on a target’s system. User involvement is required to activate GRP files; typically they are attached to a harmless-appearing e-mail message.

<table>
<thead>
<tr>
<th>Attack Name</th>
<th>Attack Description</th>
<th>Severity</th>
<th>Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP:EXT:DOT-GRP</td>
<td>This signature detects GRP files sent over SMTP. GRP files can contain Windows Program Group information, and may be exploited by malicious users to deposit instructions or arbitrary code on a target’s system. User involvement is required to activate GRP files; typically they are attached to a harmless-appearing e-mail message.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
</tbody>
</table>

## SMTP:EXT:DOT-HLP
This signature detects email attachments that have the extension `.hlp` and sent received via SMTP. Because `.HLPs` (Help File) files can contain macros, this may indicate an incoming email virus. Attackers may create malicious scripts, tricking users into executing the macros and infecting the system.

## SMTP:EXT:DOT-HT
This signature detects email attachments with the extension `.ht` sent via SMTP. This may indicate an incoming email virus or other attack. HT files contain configuration information for the Hyperterm console program, shipped with every Windows operating system since Windows 95. It is the default handler program for `.ht` files. A recent vulnerability in Hyperterm could allow an attacker to take control of your computer via an infected `.ht` file. These files are not normally sent via email.

## SMTP:EXT:DOT-INF
This signature detects email attachments that have the extension `.inf` and were sent via SMTP. Because `.INFs` (Setup Information) files contain scripts, this may indicate an incoming email virus. Attackers may create malicious scripts, tricking users into executing the file and infecting the system.

## SMTP:EXT:DOT-INS
This signature detects email attachments that have the extension `.ins` and were sent via SMTP. Because `.INSs` (Internet Naming Service) files contain configuration parameters, this may indicate an incoming email virus. Attackers may include malicious configurations, tricking users into executing the file and infecting the system.

## SMTP:EXT:DOT-ISP
This signature detects email attachments that have the extension `.isp` and were sent via SMTP. Because `.ISPs` (Internet Communication Settings) files contain configuration parameters, this may indicate an incoming email virus. Attackers may include malicious configurations, tricking users into executing the file and infecting the system.

## SMTP:EXT:DOT-JS
This signature detects email attachments that have the extension `.js` and were sent via SMTP. Because `.JSs` (JavaScript File) files contain scripts, this may indicate an incoming email virus. Attackers may create malicious scripts, tricking users into executing the file and infecting the system.

## SMTP:EXT:DOT-JSE
This signature detects email attachments that have the extension `.jse` and were sent via SMTP. Because `.JSEs` (JavaScript Encoded) files contain scripts, this may indicate an incoming email virus. Attackers may create malicious scripts, tricking users into executing the file and infecting the system.
<table>
<thead>
<tr>
<th>Attack Name</th>
<th>Attack Description</th>
<th>Severity</th>
<th>Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP:EXT:DOT-LNK</td>
<td>This signature detects email attachments that have the extension .lnk and were sent via SMTP. Because .LNKs (Windows link) files can point to any program, this may indicate an incoming email virus. Attackers may create a link pointing to a dangerous program, tricking users into executing the link and affecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-MDB</td>
<td>This signature detects email attachments that have the extension .mdb and were sent via SMTP. Because .MDBs (MS Access Application) files can contain scripts, this may indicate an incoming email virus. Attackers may create malicious scripts, tricking users into executing the file and infecting the system.</td>
<td>low</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-MDE</td>
<td>This signature detects email attachments that have the extension .mde and were sent via SMTP. Because .MDEs (Microsoft Access MDE database) files can contain scripts and macros, this may indicate an incoming email virus. Attackers may create malicious scripts, tricking users into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-MSC</td>
<td>This signature detects email attachments that have the extension .msc and were sent via SMTP. Because .MSCs (Microsoft Common Console Document) files can contain configuration information, this may indicate an incoming email virus. Attackers may change the configuration to point to a dangerous command, tricking users into executing the files and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-MSI</td>
<td>This signature detects email attachments with the extension .msi sent via SMTP. This may indicate an incoming email virus. .MSIs (Microsoft Windows Installer Package) contain executable code. Attackers may create malicious executables, tricking the user into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-MSP</td>
<td>This signature detects email attachments with the extension .msp sent via SMTP. This may indicate an incoming email virus. .MSPs (Microsoft Windows Installer Patch) contain executable code. Attackers may create malicious executables, tricking the user into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-OCX</td>
<td>This signature detects email attachments that have the extension .ocx and were sent via SMTP. Because .OCXs (Object Control Extension) files can contain multiple scripts, this may indicate an incoming email virus. Attackers may create malicious executables, tricking users into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-PCD</td>
<td>This signature detects email attachments that have the extension .pcd and were sent via SMTP. Because .PCDs (Photo CD MS Compiled Script) files can contain scripts, this may indicate an incoming email virus. Attackers may create malicious scripts, tricking users into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-PIF</td>
<td>This signature detects email attachments with the extension '.pif' sent via SMTP. This may indicate an incoming email virus. PIFs (Program Information Files) are standard Microsoft Windows files that contain start up properties for DOS applications. Attackers may hide malicious executables within a PIF file, tricking users into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-REG</td>
<td>This signature detects email attachments that have the extension <code>.reg</code> and were sent via SMTP. Because .REGs (Registry Entries) files contain entries for the Registry, this may indicate an incoming email virus. Attackers may create malicious entries, tricking users into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-SCR</td>
<td>This signature detects email attachments with the extension <code>.scr</code> sent via SMTP. This may indicate an incoming email virus. SCRs (ScreenSaver files) are renamed <code>.exe</code> files containing executable code. Attackers may disguise malicious executables to appear as harmless screensaver files, tricking the user into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-SCT</td>
<td>This signature detects email attachments with the extension <code>.sct</code> sent via SMTP. This may indicate an incoming email virus. .SCTs (Windows Script Component) contain scripts. Attackers may create malicious scripts, tricking the user into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-URL</td>
<td>This signature detects email attachments with the extension <code>.url</code> sent via SMTP. This may indicate an incoming email virus. .URLs (Internet Shortcut) contain a link to a web location. Attackers may create a malicious shortcut, tricking the user into executing the file and send the user to a malicious website.</td>
<td>low</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-VB</td>
<td>This signature detects email attachments with the extension <code>.vb</code> sent via SMTP. This may indicate an incoming email virus. .VBs (VBScript File) contain scripts. Attackers may create malicious scripts, tricking the user into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-VBS</td>
<td>This signature detects email attachments with the extension <code>.vbs</code> sent via SMTP. This may indicate an incoming email virus. VBSs (Visual Basic files) contain one or more executable scripts. Attackers may create malicious VB files, tricking the user into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-WMF</td>
<td>This signature detects metafiles (files with <code>.emf</code> or <code>.wmf</code> extensions) in an email attachment. Some versions of Microsoft Windows produce boundary errors when processing metafiles, enabling attackers to create a denial of service (DoS) and execute arbitrary code.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-WSC</td>
<td>This signature detects email attachments with the extension <code>.wsc</code> sent via SMTP. This may indicate an incoming email virus. .WSCs (Windows Script Component) contain scripts. Attackers may create malicious scripts, tricking the user into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-WSF</td>
<td>This signature detects email attachments with the extension <code>.wsf</code> sent via SMTP. This may indicate an incoming email virus. .WSFs (Windows Script File) contain scripts. Attackers may create malicious scripts, tricking the user into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-------------</td>
<td>--------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-WSH</td>
<td>This signature detects email attachments with the extension .wsh sent via SMTP. This may indicate an incoming email virus. WSHs (Windows Script Host Settings File) contain configuration parameters. Attackers may create malicious configurations, tricking the user into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXT:JOB</td>
<td>This signature detects an attached Microsoft Task Scheduler (.job) file. Opening a malicious .job file in Task Scheduler may allow for arbitrary code execution, leading to system compromise. This vulnerability is present in Microsoft Windows 2000 Service Pack 2 and later. It is also present in Microsoft Windows XP Service Pack 1.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:IIS:IIS-ENCAPS-RELAY</td>
<td>This signature detects attempts to exploit a vulnerability in the Microsoft SMTP Service in Microsoft IIS. Versions 4.0 and 5.0 are vulnerable. A maliciously crafted 'rcpt to:' command can circumvent email relaying rules. Attackers may impersonate trusted emails or send spam anonymously.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>SMTP:INVALID:2MANY-BOUNDARY</td>
<td>This protocol anomaly is an SMTP boundary depth that exceeds the user-defined maximum. The boundary depth indicates the number of nested attachments in a MIME multipart message. The default boundary depth is 4.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:INVALID:BASE64-CHAR</td>
<td>This protocol anomaly is an SMTP message with base64 encoding that contains an invalid character.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:INVALID:BOUNDARY-MISS</td>
<td>This protocol anomaly is an SMTP message with a content-type multipart that has no boundary parameter. The boundary parameter specifies a text string that is used to delimit the parts of the multipart message.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:INVALID:DUP_AUTH</td>
<td>This protocol anomaly is multiple AUTH commands within a single SMTP transaction.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:INVALID:DUP-BOUNDARY</td>
<td>This protocol anomaly is an SMTP message with a MIME multipart content-type that uses duplicate boundaries.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:INVALID:UNFIN-MULTIPART</td>
<td>This protocol anomaly is an SMTP message with a MIME multipart boundary that exceeds actual multipart data (all data is processed but unfinished boundary delimiters exist).</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:MAJORDOMO:COMMAND-EXEC</td>
<td>This signature detects attempts to send shell commands via an SMTP email message by exploiting the back-tick (') vulnerability in Great Circle Associates Majordomo, a perl-based Internet email list server. When processing a list command, Majordomo compares the &quot;reply to&quot; email address again the advertise/noadvertise lists (if configured). During this comparison, Majordomo may be tricked into executing commands when it expands the back-tick operator (used by UNIX to enclose executable commands in a shell command line). Attackers may use the back-tick operator in the &quot;reply to&quot; email header to execute arbitrary commands on the server.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>SMTP:MALACROBAT:UUEXEC</td>
<td>This signature detects a maliciously crafted PDF file attached to an email. Attackers may insert certain shell metacharacters at the beginning of a uuencoded PDF file to force Adobe Acrobat to execute arbitrary commands upon loading the file.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>SMTP:MAL:EMAIL-URL-HIDING-ENC</td>
<td>This signature detects attempts to exploit a vulnerability in Microsoft Outlook Express. Attackers may embed binary control characters in a URL that is included in an email; when the URL is viewed, these control characters prevent Outlook Express and Internet Explorer from displaying the complete URL, which may have malicious content.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:MAL:NOTES-BIGMAIL</td>
<td>This signature detects large email messages (&gt; 12 MB) sent to Lotus Domino servers via a commonly published exploit. Attackers may cause Lotus Domino to exhaust all system memory and cause the service to stop responding.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:MAL:OUTLOOK-MAILTO-QUOT</td>
<td>This signature detects attempts to exploit a vulnerability in the Outlook 2002 mail client. Attackers may use mailto: URLs that contain &amp;quot; strings to execute arbitrary script commands, enabling them to execute code remotely.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:MAL:SQM-CONTENT-XSS</td>
<td>This signature detects attempts to exploit a vulnerability in SquirrelMail, a PHP4 Webmail package. Attackers may send email messages that contain Javascript in the Content-Type field; when SquirrelMail receives the message, it may interpret and execute the Javascript, enabling the attacker to compromise the target system.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>SMTP:MDAEMON:SEND-OF</td>
<td>This signature detects buffer overflow attempts against the MDaemon mail server. MDaemon 6.7.9 and older versions are vulnerable. Attackers may send an overly long SMTP SAML, SOML, or SEND command to overflow the buffer and crash the MDaemon service; attackers may also obtain complete control of the server with SYSTEM level access.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:MSSQL-WORM-EMAIL</td>
<td>This signature detects attempts to send an email to <a href="mailto:ixltd@postone.com">ixltd@postone.com</a>. This may indicate the presence of SQLsnake, a MSSQL worm. SQLsnake infects Microsoft SQL Servers that have SA (administrative) accounts without passwords. The worm sends a password list and other system information via email to <a href="mailto:ixltd@postone.com">ixltd@postone.com</a>, then begins scanning for vulnerable hosts listening on TCP/1433.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>SMTP:OVERFLOW:BOUNDARY</td>
<td>This protocol anomaly is an SMTP message with a boundary length that exceeds 70 characters. The SMTP RFC specifies 70 as the maximum number of characters in a boundary.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:OVERFLOW:COMMAND-LINE</td>
<td>This protocol anomaly is a text line (in the command section, before the DATA command) in an SMTP connection that is too long. This may indicate a buffer overflow attempt.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>SMTP:OVERFLOW:CONTENT-NAME</td>
<td>This protocol anomaly is an SMTP content-type name that exceeds the user-defined maximum. The default number of bytes in a content-type name is 128.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:OVERFLOW:EMAIL-ADDRESS</td>
<td>This protocol anomaly is an email address that is too long. This may indicate a buffer overflow attempt.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>SMTP:OVERFLOW:EMAIL-DOMAIN</td>
<td>This protocol anomaly is a domain name within an email address (for example, localhost.localdomain in <a href="mailto:root@localhost.localdomain">root@localhost.localdomain</a>) that is too long. This may indicate a buffer overflow attempt.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>SMTP:OVERFLOW:EMAIL-USERNAME</td>
<td>This protocol anomaly is a user name within an email address (for example, root in <a href="mailto:root@localhost.localdomain">root@localhost.localdomain</a>) that is too long. This may indicate a buffer overflow attempt.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>-----------</td>
</tr>
<tr>
<td>SMTP:OVERFLOW:FILENAME</td>
<td>This protocol anomaly is an SMTP content-disposition filename that exceeds the user-defined maximum. The default number of bytes in a content-disposition filename is 128.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:OVERFLOW:METAMAIL-HDR-FS2</td>
<td>This signature detects SMTP messages with headers that contain format string errors. Metamail 2.7 and earlier versions are vulnerable. Because Metamail does not handle SMTP headers correctly, attackers may send maliciously crafted SMTP messages to execute arbitrary code at the same privilege level as the target (typically user). Note: Systems that typically carry non-English email messages should not include this attack object in their Security Policy.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:OVERFLOW:METAMAIL-HDR-OF1</td>
<td>This signature detects SMTP messages with large headers that contain character set information. Metamail 2.7 and earlier versions are vulnerable. Because Metamail does not handle SMTP headers correctly, attackers may send maliciously crafted SMTP messages to execute arbitrary code at the same privilege level as the target (typically a user). Note: Systems that typically carry non-English email messages should not include this attack object in their Security Policy.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:OVERFLOW:METAMAIL-HDR-OF2</td>
<td>This signature detects SMTP messages with large headers that contain character set information. Metamail 2.7 and earlier versions are vulnerable. Because Metamail does not handle SMTP headers correctly, attackers may send maliciously crafted SMTP messages to execute arbitrary code at the same privilege level as the target (typically a user). Note: Systems that typically carry non-English email messages should not include this attack object in their Security Policy.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:OVERFLOW:OUTLOOK-CERT-OF</td>
<td>This signature detects attempts to exploit a vulnerability in Sendmail. Sendmail versions 5.79 to 8.12.7 are vulnerable. Attackers may include multiple empty address containers in an SMTP header field to overflow the SMTP header buffer and force Sendmail to execute arbitrary code on the host; attackers may obtain root access.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>SMTP:OVERFLOW:REPLY-LINE</td>
<td>This protocol anomaly is a server reply line in an SMTP connection that is too long. This may indicate a buffer overflow attempt by a compromised or malicious SMTP server.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>SMTP:OVERFLOW:SENDMAIL-CMT-OF1</td>
<td>This signature detects attempts to exploit a vulnerability in Sendmail. Sendmail versions 5.79 to 8.12.7 are vulnerable. Attackers may include multiple empty address containers in an SMTP header field to overflow the SMTP header buffer and force Sendmail to execute arbitrary code on the host; attackers may obtain root access.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>SMTP:OVERFLOW:SENDMAIL-CMT-OF2</td>
<td>This signature detects attempts to exploit a vulnerability in Sendmail. Sendmail versions 5.79 to 8.12.7 are vulnerable. Attackers may include multiple empty address containers in an SMTP header field to overflow the SMTP header buffer and force Sendmail to execute arbitrary code on the host; attackers may obtain root access.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>SMTP:OVERFLOW:SENDMAIL-MIME-OF</td>
<td>This signature detects buffer overflow attempts against Sendmail. Sendmail versions 8.8.0 and 8.8.1 are vulnerable. Attackers may embed a maliciously crafted MIME header in an email to overflow a buffer in Sendmail and execute arbitrary commands as root.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>-----------</td>
</tr>
<tr>
<td>SMTP:OVERFLOW:SQRLMAIL-HDR-INJ</td>
<td>This signature detects SMTP messages with Base-64 encoded headers. SquirrelMail 1.4.3a and earlier versions do not correctly sanitize SMTP headers. Attackers may send maliciously crafted SMTP messages to execute arbitrary code at the same privilege level as the target (typically user). Note: Systems that typically carry non-English email messages should not include this attack object in their Security Policy.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:OVERFLOW:TOO-MANY-RECP</td>
<td>This protocol anomaly is too many 'RCPT TO:' recipients in an SMTP connection. This may indicate a very popular email message or a DoS/buffer overflow attempt.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>SMTP:REQERR:REQ-SYNTAX-ERROR</td>
<td>This protocol anomaly is an unparsed SMTP command line or header line due to a missing ':'. This may indicate a non-standard email client or server or a backdoor/exploit attempt.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:RESPONSE:PIPE-FAILED</td>
<td>This signature detects SMTP server responses that are generated when an unsuccessful attempt is made to send shell commands via an SMTP email message by exploiting the pipe ('</td>
<td>') passthrough vulnerability in SendMail. If the '</td>
<td>' operator was used within specified &quot;mail to&quot; and/or &quot;rcpt to&quot; email addresses to cause Sendmail to reroute data to another program, attackers receive a '550' error message.</td>
</tr>
<tr>
<td>SMTP:SAGTUBE-DOS</td>
<td>This signature detects character strings within an email message that are designed to exploit a vulnerability in SpamAssassin. SpamAssassin Project SpamAssassin 2.63 and earlier are vulnerable. SpamAssassin uses a weighting system to determine when an email message is spam. Attackers may send a maliciously crafted email with a spoofed address to cause SpamAssassin to consider all further email from the spoofed address as spam, regardless of the target's whitelist settings. After the malicious email has been received by the target, SpamAssassin blocks all emails from the spoofed address.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:SENDMAIL:ADDR-PRESCAN-ATK</td>
<td>This signature detects attempts to exploit a vulnerability in Sendmail SMTP server versions prior to 8.12.9. Because the prescan() procedure that processes email addresses in SMTP headers does not perform some char and int conversions correctly, attackers may send a maliciously crafted request to corrupt the Address Prescan Memory on a Sendmail SMTP server and execute arbitrary code.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>SMTP:SENDMAIL:SENDMAIL-FF-OF</td>
<td>This signature detects attempts to exploit a vulnerability in Sendmail versions 8.12.8 and earlier. Under certain conditions, the Sendmail address parser does not perform sufficient bounds checking when converting char to int. Attackers may use this exploit to gain control of the server.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>TROJAN:AUTOPROXY:INFECTED-HOST</td>
<td>This signature detects the AutoProxy trojan attempting to contact a master server and register the IP address and open ports of the infected host. AutoProxy is a trojan that installs a proxy server on Microsoft Windows hosts. Attackers may use an infected host to attack other targets while masking their actual IP address.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>TROJAN:MISC:MOONPIE3-FTP-RESP</td>
<td>This signature detects a banner from the FTP server embedded in the MoonPie backdoor version 3.0 (other versions may also be detected).</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>TROJAN:MISC:WANREMOTE-ADMIN</td>
<td>This signature detects access to the WanRemote administration interface using the HTTP protocol.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>TROJAN:MS-04-028:BACKDOOR-LOGIN</td>
<td>This signature detects login attempts from a client infected with a trojan installed as part of the Microsoft GDI+ Library JPEG overflow exploit.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>TROJAN:MS-04-028:TOOL-DOWNLOAD</td>
<td>This signature detects attempts by a specific trojan to download files. The trojan, installed as part of the Microsoft GDI+ Library JPEG Overflow exploit, is attempting to download updated files from a remote host.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>TROJAN:PHATBOT:FTP-CONNECT</td>
<td>This signature detects Phatbot FTP connections. Phatbot, a trojan similar to Agobot but with more functionality, sends spam from an infected host machine.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>TROJAN:QAZ:TCP25-CALLING-HOME</td>
<td>This signature detects the string 'nongmin.cn' within an SMTP header-from field sent from a remote system to local server port 25. This may indicate an attacker is attempting to access the Trojan/Worm QAZ. The QAZ Trojan/Worm, famous for infecting the Microsoft network October 2000, allows attackers to access data and gain control over some functions on remote Microsoft Windows systems.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:POP3:BABYLONIA</td>
<td>This signature detects email attachments with the file name 'x-mas.exe' sent via POP3. This may indicate the Babylonia email virus is attempting to enter the system. The executed virus infects all files greater than 8kb, installs automatic virus updaters, and allows attackers to further compromise the system by uploading trojans, creating backdoors, etc.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:POP3:BADASS</td>
<td>This signature detects email attachments with the file name 'badass.exe' sent via POP3. This may indicate the BadAss email virus is attempting to enter the system. The executed virus displays a message box with specified text, opens the Microsoft Outlook database, and sends infected messages containing a Dutch phrase to all addresses found.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:POP3:EICAR-ATTACHMENT</td>
<td>This signature detects the EICAR antivirus test file sent as an email attachment.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:POP3:EUROCALCULATOR</td>
<td>This signature detects email attachments with the file name 'Eurocalculator.exe' sent via POP3. This may indicate the Eurocalculator Trojan is attempting to enter the system. The executed file installs a remote administration Trojan similar to Back Orifice, allowing attackers to access data and gain control over some functions on remote Microsoft Windows systems.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:POP3:EXPLOREZIP-B</td>
<td>This signature detects email attachments with the file name 'zippati.exe' sent via POP3. This may indicate the email virus ExploreZip.B is attempting to enter the system. The executed ZIP file (zippati in Italian) installs the program explore.exe, which edits the host and visible networked WIN.INI files to run explore.exe on startup. The virus also searches all local and visible networked drives for common file types (.ASN, .C, .CPP, .DOC, .H, .XLS, .PPT) and reduces them to zero bytes.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>VIRUS:POP3:FIX2001</td>
<td>This signature detects email attachments with the file name 'fix2001.exe' sent via POP3. This may indicate the email virus Fix2001 is attempting to enter the system. The executed file edits the Registry to run the virus on startup, obtains email addresses from sent and received messages, and sends infected email messages to all addresses found. If the virus is patched or corrupted, it also overwrites the C:COMMAND.COM file with a denial-of-service (DoS) (DoS) trojan that erases all drive data upon reboot.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:POP3:FREELINK</td>
<td>This signature detects email attachments named 'Link.vbs' sent via POP3. This may indicate the VBS.Freelink email virus is attempting to enter the system. The executed virus edits Microsoft Windows Registry entries, opens the Microsoft Outlook database, and sends infected messages to all addresses found.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:POP3:HAPPY99</td>
<td>This signature detects emails with the header 'X-Spanska: Yes' and the UU-encoded attachment 'Happy99.exe' sent via POP3. This may indicate the email virus/worm Happy99/Ska is attempting to enter the system. The executed file edits files (notably WSOCK32.DLL) in the system directory, obtains email addresses from sent and received messages, and sends infected email messages to all addresses found. Once WSOCK32.DLL is successfully modified, the virus/worm also exhibits a message box animation routine of a fireworks display.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:POP3:IROK</td>
<td>This signature detects email attachments named 'irok.exe' sent via POP3. This may indicate the email virus Irok is attempting to enter the system. The executed file exhibits a message box animation routine of a starfield while copying itself to the Windows system directory and writing the file Irokrun.vbs to the Startup directory. Upon reboot, the VB script uses Windows Scripting Host (WSH) to open the Microsoft Outlook database and send infected files to up to 60 addresses found. This virus also install the file script.ini to the m IRC directory and use dcc to send irok.exe to IRC clients who join the channel.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:POP3:MATRIX</td>
<td>This signature detects emails with the content 'Software provided by Matrix' sent via POP3. This may indicate the email virus Matrix is attempting to enter the system. The executed file first checks for antivirus software running on the host and terminates if found. Otherwise, the virus copies itself to the Windows directory as ie_pack.exe, runs, and renames to Win32.dll. Matrix also installs the downloader program Mtx_.exe (which downloads plug-ins for the virus upon reboot), and infects Win32 executables.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:POP3:MYPICS</td>
<td>This signature detects email attachments named 'pics4you.exe' sent via POP3. This may indicate the email virus MyPics is attempting to enter the system. The executed file installs as Pics4You.exe and writes itself to the Windows Startup directory, obtains email addresses from the Microsoft Outlook database, and sends infected email messages to 50 addresses at a time. MyPics was also designed to corrupt CMOS data and reformat hard drives on 1/1/2000.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>VIRUS:POP3:MYROMEO-BLE-BLA</td>
<td>This signature detects emails with the subject 'ble bla' with the attachments myjuliet.chm and myromeo.exe sent via POP3. This may indicate the email virus Verona is attempting to enter the system. Because CHM files are compressed HTML files, myjuliet.chm is activated when viewed in the Microsoft Outlook preview pane; once triggered, the CHM file runs myromeo.exe in the background. Myromeo.exe obtains email addresses from the Microsoft Outlook database, sends infected email messages to all addresses found, and edits the Window directory file hh.dat.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:POP3:MYROMEO-EXE</td>
<td>This signature detects email attachments with the name 'myromeo.exe' accompanied by myjuliet.chm and sent via POP3. This may indicate the email virus Verona is attempting to enter the system. Because CHM files are compressed HTML files, myjuliet.chm is activated when viewed in the Microsoft Outlook preview pane; once triggered, the CHM file runs myromeo.exe in the background. Myromeo.exe obtains email addresses from the Microsoft Outlook database, sends infected email messages to all addresses found, and edits the Window directory file hh.dat.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:POP3:MYROMEO-I-LOVE-YOU</td>
<td>This signature detects emails with the attachments myjuliet.chm and myromeo.exe sent via POP3. This may indicate the email virus Verona is attempting to enter the system. Because CHM files are compressed HTML files, myjuliet.chm is activated when viewed in the Microsoft Outlook preview pane; once triggered, the CHM file runs myromeo.exe in the background. Myromeo.exe obtains email addresses from the Microsoft Outlook database, sends infected email messages to all addresses found, and edits the Window directory file hh.dat.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:POP3:MYROMEO-MYJULIET</td>
<td>This signature detects email attachments with the name 'myjuliet.chm' accompanied by myromeo.exe and sent via POP3. This may indicate the email virus Verona is attempting to enter the system. Because CHM files are compressed HTML files, myjuliet.chm is activated when viewed in the Microsoft Outlook preview pane; once triggered, the CHM file runs myromeo.exe in the background. Myromeo.exe obtains email addresses from the Microsoft Outlook database, sends infected email messages to all addresses found, and edits the Window directory file hh.dat.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:POP3:NAVIDAD</td>
<td>This signature detects email attachments named 'navidad.exe' sent via POP3. This may indicate the email virus Navidad is attempting to enter the system. The executed file copies itself as winsrvc.vxd to the Windows system directory and edits the Registry to run the virus on reboot, installs into the system tray, and displays a dialog box with the text 'Ul.' The virus also intercepts new incoming email addresses and sends infected email messages to all senders.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>VIRUS:POP3:NIMDA</td>
<td>This signature detects email attachments named ‘readme.exe’ sent via POP3. This may indicate the email virus Nimda is attempting to enter the system. The executed file installs to the Windows directory, edits the Registry to run the virus on reboot, and infects Internet-related files. Nimda then obtains email addresses and sends infected messages to all addresses found using its own SMTP server.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:POP3:PAPA</td>
<td>This signature detects email attachments named ‘xpass.xls’ sent via POP3. This may indicate the email virus Papa is attempting to enter the system. The executed Microsoft Excel file obtains email addresses from Microsoft Outlook database and sends infected messages to the first 60 addresses found. Papa also attempts to create a denial-of-service (DoS) by pinging the all.net Web server.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:POP3:PASSION</td>
<td>This signature detects email attachments named ICQ_Greeting.exe sent using POP3. This may indicate the email virus Passion is attempting to enter the system. The executed file copies itself to local root drive, edits the registry to run the virus on reboot, and deletes files. Passion then obtains email addresses from the Microsoft Outlook database and sends infected messages to the first 50 addresses found.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:POP3:PIKACHU-POKEMON</td>
<td>This signature detects emails with the subject ‘Pikachu Pokemon’ sent via POP3. This may indicate the email virus Pikachu Pokemon is attempting to enter the system. The executed file displays a “friendly” message featuring Pikachu while it overwrites the Autoexec.Bat file to delete most Microsoft Windows 9x system files upon reboot. Pikachu then obtains email addresses from Microsoft Outlook database and sends infected messages to all addresses found.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:POP3:PRETTY-PARK</td>
<td>This signature detects emails with the subject ‘C:\CoolProgs\Pretty Park.exe’ sent via POP3. This may indicate the email virus Pretty Park is attempting to enter the system. The executed file copies itself to the Windows System directory as FILES32.VXD and edits the Registry to run the virus on reboot. Pretty Park then obtains email addresses from Microsoft Outlook database and sends infected messages to all addresses found every 30 minutes. The virus also attempts to contact its author via IRC chat every 30 seconds; attackers may use the installed virus as a backdoor remote access tool to further compromise the system.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:POP3:SIMBIOSIS</td>
<td>This signature detects email attachments named ‘SETUP.EXE’ sent via POP3. This may indicate the email virus Simbiosis (Cholera worm executable containing a CTX virus) is attempting to enter the system. The executed Cholera worm copies itself to the Windows directory and edits either the WIN.INI file (Windows 9x) or the Registry (NT) to run the virus on reboot. Simbiosis then obtains email addresses from Internet-related files and sends infected messages to all addresses found using its own SMTP server. The executed CTX virus appends and infects Microsoft Windows PE executables; the virus does not carry a payload and is apparent only through a video effect.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>VIRUS:POP3:SUPPL</td>
<td>This signature detects email attachments named 'Suppl.doc' sent via POP3. This may indicate the email virus/trojan Suppl is attempting to enter the system. The executed file macros copy the active (virus) document to the Windows directory as Anthrax.ini and decompress the malicious Wsock32.dll file appended to Suppl.doc. On reboot, the virus file DLL.tmp replaces the malicious Wsock32.dll and the original Wsock32.dll is renamed to Wsock33.dll. Suppl then attaches to all outgoing SMTP email messages, locates files with common extensions (DOC, .TXT, .ZIP, etc) on available hard drives, and truncates those files to zero bytes.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:POP3:THEFLY</td>
<td>This signature detects email attachments named 'The_Fly.chm' sent via POP3. This may indicate the email virus The Fly is attempting to enter the system. The executed file copies itself as THE_FLY.CHM to the Windows directory, as DXGFXB3D.DLL to Windows system directory, and opens a graphic with message 'If you ride a motorcycle, close your mouth'. The Fly then copies MSJSVM.JS to the Windows system directory and edits the Registry to run this JavaScript upon reboot. The virus also obtains email addresses from the Microsoft Outlook database and sends infected messages to all addresses found.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:POP3:TIMOFONICA</td>
<td>This signature detects email attachments named 'Timofonica.txt.vbs' sent via POP3. This may indicate the email virus Timofonica is attempting to enter the system. The executed file creates cmos.com and edits the Registry to run the virus on reboot. When cmos.com is run, it erases CMOS memory, MBRs from the first four physical hard disks, and MBRs and DOS Boot Records of extended partitions. Timofonica also obtains email addresses from the Microsoft Outlook database and sends infected messages to all addresses found. Simultaneously, the virus emails the SMS gateway at Moviestar.net and send SMS messages to random cellular phone numbers.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:POP3:TOADIE</td>
<td>This signature detects email attachments named 'Toadie.exe' sent via POP3. This may indicate the email virus Toadie is attempting to enter the system. The executed file infects EXE files by relocating the initial 7800 bytes to the end of the file, encrypting those bytes, and writing 7800 bytes of its own DOS program to the beginning of the file, thus changing EXE files to DOS files. When run, the virus code first infects more EXE files before passing control. Toadie also replaces unsent email messages in Pegasus Mail, and may send copies of itself via IRC.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>VIRUS:POP3:TRIPLESIX</td>
<td>This signature detects email attachments named '666test.vbs' sent via POP3. This may indicate the email virus TripleSix is attempting to enter the system. The executed file displays three dialogue boxes leading the user through the game &quot;Does your name add up to 666?&quot;. The virus then copies WINTEMP.TXT to the Windows directory; this file creates WINITMP.EXE (a PkZip executable), which in turn creates 666TEST.ZIP (an archive). The archive is copied to the Windows system directory as WINSWAP.SWP. Triplesix also writes REGSVR.VBS to the Windows system directory and edits the Registry to run that script on reboot. When REGSVR.VBS is activated, it obtains email addresses from the Microsoft Outlook database and sends infected messages to all addresses found, overwrites mIRC and Pirch setup files, and sends infected messages via IRC.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:POP3:TUNE</td>
<td>This signature detects email attachments named 'Tune.vbs' sent via POP3. This may indicate the email virus Tune is attempting to enter the system. The executed file copies itself to the Windows, Windows system, and Temporary directories and edits the Registry to run the virus on reboot. When activated, it obtains email addresses from the Microsoft Outlook database and sends infected messages to all addresses found, overwrites mIRC and Pirch setup files, and sends infected messages via IRC.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:POP3:UENCODED-DOT-VBS</td>
<td>This signature detects email attachments containing the string 'begin' and the file extension 'vbs' sent via POP3. This may indicate the email virus LoveLetter is attempting to enter the system. The executed file copies itself to the Windows system directory and edits the Registry to run the virus on reboot; when activated, it downloads a trojan from a specified web site that deletes security keys and sends stolen passwords to its owner. LoveLetter also obtains email addresses from the Microsoft Outlook database and sends infected messages to all addresses found, overwrites mIRC and Pirch setup files, and sends infected messages via IRC.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:POP3:WSCRIPT-KAK</td>
<td>This signature detects emails containing 'kak.hta' sent via POP3. This may indicate the email virus Kak is attempting to enter the system. The virus arrives embedded within Microsoft Outlook message signature file as kak.htm, and activates when viewed in the Microsoft Outlook preview pane. Once triggered, the file copies itself as kak.ha to the Windows startup and system directories; on reboot, the virus overwrites the autoexec.bat file to delete the virus from the startup directory. Kak then replaces the Microsoft Outlook message signature with infected file kak.htm. The virus also displays an alert box after 6pm on the first day of the month and shows down Windows.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:POP3:Y2K-ZELU</td>
<td>This signature detects email attachments named 'Y2k.exe' sent via POP3. This may indicate the email virus Zelu is attempting to enter the system disguised as the utility ChipTec Y2K Freeware Version. The executed file scans available directories, corrupts writeable files, and inserts a message at the beginning of infected files. Zelu may reset the system, making the operating system unusable and erasing all data.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>VIRUS:POP3:ZIPPED</td>
<td>This signature detects email attachments named ‘ZippedFiles.exe’ sent via POP3. This may indicate the email virus Zipped Files is attempting to enter the system. The executed ZIP file installs the program explore.exe, which edits the host and visible networked WIN.INI files to run explore.exe on startup. The virus also searches all local and visible networked drives for common file types (.ASN, .C, .CPP, .DOC, .H, .XLS, .PPT) and reduces them to zero bytes.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:SMTP:BAGLE:Q-SMTP</td>
<td>This signature detects the Q through T variants of the Bagle SMTP virus. Bagle sends emails containing an attachment with a malicious payload. Viewing the email message loads an external link using HTTP; this link is actually an executable program that infects the target. The virus then sends a copy of itself to email addresses found on the target’s hard drive using the target’s email address as the return address.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:SMTP:DOUBLE-DOT-DOT</td>
<td>This signature detects email attachments that contain two file extensions. Attackers or viruses may send email attachments that use two file extensions to disguise the actual file name and trick users into opening a malicious attachment.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:SMTP:DUMARU.J</td>
<td>This signature detects the J variant of the Dumaru SMTP virus. Dumaru sends emails with the subject line: “Important information for you. Read it immediately!”, the email includes a .zip attachment that contains a malicious payload disguised as a picture. When the picture is viewed, the malicious executable program infects the target host. The virus then sends a copy of itself to email addresses found in the target’s address book, using the target’s email address as the return address.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:SMTP:EICAR-ATTACHMENT</td>
<td>This signature detects the EICAR antivirus test file sent as an email attachment.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:SMTP:EXE-ATTACH-1</td>
<td>This signature detects Win32 executables sent as a MIME attachment. Many viruses, worms, and other malicious programs are transmitted through SMTP attachments. You might want to block all executable attachments and instead require your users to send executables in a compressed format.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:SMTP:EXE-IN-ZIP</td>
<td>This signature detects Win32 executables sent within a ZIP file as a MIME attachment. Many viruses, worms, and other malicious programs are transmitted through SMTP attachments. You might want to block all executable attachments.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:SMTP:NAIL</td>
<td>This signature detects attempts by the email virus Nail to enter the system. When executed, the virus assigns the Microsoft Word auto.dot template to a template located on an attacker Web site, enabling the attacker to upload new virus code. Nail then starts a MAP (Mail API) session, obtains email addresses from the Microsoft Outlook database, and sends infected email messages to all addresses found. Finally, the virus sends an email message to <a href="mailto:chainnail@hotmail.com">chainnail@hotmail.com</a>, assumed to be the email address of the virus author.</td>
<td>high</td>
<td>sos5.0.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>--------------</td>
</tr>
<tr>
<td>VIRUS:SMTP:RESUME-EXPLORER-DOC</td>
<td>This signature detects email attachments named ‘EXPLOREDO.DOC’ sent via SMTP. This may indicate the email virus Resume is attempting to enter the system. The executed file obtains email addresses from Microsoft Outlook database and sends infected messages to all addresses found. When the file is closed, Resume creates directory C:Data, copies itself there as Normal.dot, and edits the Registry to run the virus on reboot. The virus then attempts to delete all files from several directories (including Windows) and all drives from A: to Z.</td>
<td>low</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:SMTP:SOBIG-ATTACHMENTS</td>
<td>This signature detects email attachments with one of the following file name sent via SMTP: approved.pif, application.pif, doc_details.pif, movie28.pif, password.pif, ref-39xxxx.pif, screen_doc.pif, screen_temp.pif, _approved.pif. This may indicate the SOBIG email virus is attempting to enter the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VOIP:MGMT:XPRESSA-HTTP-DOS</td>
<td>This signature detects attempts to exploit a vulnerability in Pingel Xpressa phones. Attackers may supply an overly long request to the HTTP management server on the phone to execute arbitrary code or crash the phone (the phone must be rebooted).</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>WORM:AGOBOT:HTTP-SHARE-ENUM</td>
<td>This signature detects attempts by the Agobot worm to enumerate SMB shares via HTTP.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>WORM:AGOBOT:PY-HTTP-PROP</td>
<td>This signature detects the PY variant of the Agobot worm as it attempts to infect another host. This signature could be prone to false positives.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>WORM:BAGLE:AF-HTTP</td>
<td>This signature detects the AF variant of the Bagle SMTP virus. Bagle sends emails that contain an attachment with a malicious payload. When the attachment is viewed, the payload uses HTTP to load an external link, which is actually an executable program that infects the target host. The virus then sends a copy of itself to email addresses found on the target’s hard drive, using the target’s email address as the return address.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>WORM:BAGLE:AF-SMTP</td>
<td>This signature detects the AF variant of the Bagle SMTP virus. Bagle sends emails to victims with an attachment with malicious payload. Attempting to view the attachment, which is actually an executable program, infects the user. The virus then sends a copy of itself to emails found searching the victim’s hard drive for addresses, with the victim’s email address as the return address.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>WORM:BERBEW:KEYLOGGER-UPLOAD</td>
<td>This signature detects the Berbew worm as it uploads keylogger information to a listening post. Berew monitors user keystrokes for financial data and reports that information to an attacker via HTTP to a listening post. Source IP addresses that trigger this signature are extremely likely to be infected with the Berbew worm.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>WORM:BOBAX:C-PHONE-HOME-DNS</td>
<td>This signature detects Bobax worm activity. The C variant of the Bobax worm attempts to lookup the correct IP addresses for listening post servers set up by the Bobax virus authors. Because lookups for these addresses are extremely suspicious, you should investigate the source device for Bobax infection. However, this signature detects Bobax activity (not Bobax infection attempts), and cannot be used to prevent Bobax infection. To prevent Bobax infection, configure your Security Policy to drop traffic that matches the signatures &quot;Windows RPC: LSASS Malicious OpCode&quot; and &quot;Windows RPC: LSASS DCE-RPC Oversized Fragment&quot;.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>WORM:CODERED:INFECTION-ATTEMPT</td>
<td>The signature detects attempts to infect an Microsoft IIS server with the Code Red worm using a .ida buffer-overflow attack. The installed worm downloads code from the donor host, creates a backdoor on the victim, and sets up 100 threads of the worm that scan for other vulnerable hosts using random IP addresses. Code Red also checks the host system time; on the 20th of each month (GMT), all infected systems send 100k bytes of data to TCP/80 of <a href="http://www.whitehouse.gov">www.whitehouse.gov</a>, causing a denial-of-service (DoS).</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>WORM:CODERED-2:CMD-BACKDOOR</td>
<td>This signature detects attempts to access a backdoor web script installed by the Code Red II worm. The Code Red II worm, like the original Code Red worm, allows attackers to remotely access the server.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>WORM:CODERED-2:INFECT-ATTEMPT</td>
<td>This signature detects attempts by the CodeRedII worm to infect a host. The CodeRedII worm, also known as CodeRed.F, exploits the same vulnerability as the original CodeRed worm.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>WORM:CODERED-2:ROOT-BACKDOOR</td>
<td>This signature detects attempts to access a backdoor web script installed by the Code Red II worm. The Code Red II worm, like the original Code Red worm, allows attackers to remotely access the server.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>WORM:EMAIL:BAGLE-INFECTION</td>
<td>This signature detects the Bagle worm activity on a host. After infecting a host, the Bagle worm attempts to contact a Web server listening post. The Bagle worm, which affects Microsoft Windows, copies itself to the system directory, and edits the system registry. The worm uses an email attachment to propagate itself to other hosts, and has a hard-coded expiration date (January 28). This signature could be prone to false positives.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>WORM:EMAIL:W32.SOBIG.E</td>
<td>This signature detects e-mail attachments containing the W32.Sobig.E worm sent via SMTP.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>WORM:MIMAIL:MIMAIL.A</td>
<td>This signature detects the Mimail.A worm attachment in SMTP traffic. After infecting a Windows-based host, Mimail sends itself as an attachment to another target using its own SMTP engine.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>WORM:MIMAIL:MIMAIL.L</td>
<td>This signature detects the Mimail.L worm attachment in SMTP traffic. After infecting a Windows-based host, Mimail sends itself as an attachment to another target using its own SMTP engine.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
</tbody>
</table>
### Attack Name | Attack Description | Severity | Versions  
--- | --- | --- | ---  
WORM:MOFEI:MOFEI-B-PROPAGATION | This signature detects the MoFei worm attempting to propagate to another host. After infecting a host, the MoFei worm propagates by depositing a copy of itself in a vulnerable NetBIOS folder on another host. The MoFei worm is known by several aliases, including W32.Mofei-B and W32.Femot.D. | high | sos5.1.0  
WORM:NACHI:B-C-D-INFECT-ATTEMPT | This signature detects infection attempts of the Windows RPC Locator Service by the B, C or D variants of the Nachi worm. This signature only triggers on a successful connect to an accessible victim. Follow up is strongly suggested. | critical | sos5.1.0  
WORM:NACHI:D-WEBDAV-ATK | This signature detects WebDAV overflows, which can indicate an infection attempt by the Nachi worm (D variant). Nachi.D, a worm, typically attempts to infect the target host by exploiting several vulnerabilities. | high | sos5.0.0, sos5.1.0  
WORM:NETSKY:V-SMTP-PROP | This signature detects the V variant of the NetSky worm. The V variant encodes a malicious HTML script in the body of an email sent to the target host. Due to a known vulnerability, Microsoft Outlook and Outlook Express process the encoded script when the email appears in the preview pane (the email does not need to be opened). The script downloads the NetSky worm from known Internet sites and installs the worm on the target host. | high | sos5.1.0  
WORM:NIMDA:BIN-255-CMD | This signature detects attempts to infect a Microsoft IIS Web server with the Nimda worm. Nimda may infect other Web servers by obtaining email addresses and sending a copy of itself in infected messages using its own SMTP or POP3 server; adding files to a system configured to allow Windows file shares; or posting an infected HTML email to the Web server where it can be accessed via HTTP. | medium | sos5.0.0, sos5.1.0  
WORM:NIMDA:MSADC-ROOT | This signature detects attempts to infect a Microsoft IIS Web server with the Nimda worm. Nimda may infect other Web servers by obtaining email addresses and sending a copy of itself in infected messages using its own SMTP or POP3 server; adding files to a system configured to allow Windows file shares; or posting an infected HTML email to the Web server where it can be accessed via HTTP. | medium | sos5.0.0, sos5.1.0  
WORM:NIMDA:NIMDA-EML | This signature detects attempts to create .EML files on the system, a common sign of the NIMDA worm. The worm browses remote directories and creates .EML files (the worm's multi-part messages containing a MIME-encoded worm) with the same names as existing documents or Web page files. | medium | sos5.1.0  
WORM:NIMDA:NIMDA-NWS | This signature detects attempts to create a .NWS file on the system, a common sign of the NIMDA worm. The worm browses remote directories and creates .NWS files (the worm's multi-part messages containing a MIME-encoded worm) with the same names as existing documents or Web page files. | medium | sos5.1.0  
WORM:NIMDA:NIMDA-RICHED20 | This signature detects attempts to create the file RICHED20.DLL on the system, a common sign of the NIMDA worm. The worm may overwrite the original RICHED20.DLL in the Windows systems folder with a binary copy of itself, and place additional copies in all folders containing .DOC or .EML files. | high | sos5.1.0
**Configuration Log Entries**

The Configuration category contains the following subcategories:

<table>
<thead>
<tr>
<th>Attack Name</th>
<th>Attack Description</th>
<th>Severity</th>
<th>Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>WORM:NIMDA:SCRIPTS-C1C-CMD</td>
<td>This signature detects attempts to infect a Microsoft IIS Web server with the Nimda worm. Nimda may infect other Web servers by obtaining email addresses and sending a copy of itself in infected messages using its own SMTP or POP3 server; adding files to a system configured to allow Windows file shares; or posting an infected HTML email to the Web server where it can be accessed via HTTP.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>WORM:NIMDA:SCRIPTS-CMD</td>
<td>This signature detects attempts to infect a Microsoft IIS Web server with the Nimda worm. Nimda may infect other Web servers by obtaining email addresses and sending a copy of itself in infected messages using its own SMTP or POP3 server; adding files to a system configured to allow Windows file shares; or posting an infected HTML email to the Web server where it can be accessed via HTTP.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>WORM:NIMDA:SCRIPTS-ROOT</td>
<td>This signature detects attempts to infect a Microsoft IIS Web server with the Nimda worm. Nimda may infect other Web servers by obtaining email addresses and sending a copy of itself in infected messages using its own SMTP or POP3 server; adding files to a system configured to allow Windows file shares; or posting an infected HTML email to the Web server where it can be accessed via HTTP.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>WORM:PHPINCLUDE:SEARCH-REQ</td>
<td>This signature detects the Santy.C worm attempting to find targets by sending a search request to a Google or Yahoo search engine.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>WORM:SANTY:GOOGLE-SEARCH</td>
<td>This signature detects a machine infected with the Santy worm querying Google to locate new targets for infection. The source IP of this log is likely infected with a variant of Santy.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>WORM:SANTY:INFECT-ATTEMPT</td>
<td>This signature detects a machine infected with the Santy worm attempting to infect a new target host. The source IP of this log is likely infected with a variant of Santy.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>WORM:SMB:DELODER</td>
<td>This signature detects attempts to upload the deloder worm. This signature also indicates that the worm has already logged into the system; the deloder worm can upload itself to the host only after successful login as Administrator (deloder uses one of 50 default passwords to login).</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>WORM:SMB:W32-SLACKOR</td>
<td>This signature detects SMB transmissions of the W32/Slackor worm, which targets file shares. The worm scans the /16 of the infected host for systems listening on TCP/445; if a system is found, the worm uses pre-programmed usernames and passwords to connect to the $IPC share on the system, copies itself to the C:\sp directory, and runs its payload.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
</tbody>
</table>
Table 83: Configuration Log Entries

<table>
<thead>
<tr>
<th>Configuration Log Entry Subcategories</th>
<th>ScreenOS Message ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Addresses &gt; Notification &gt; 00001</td>
</tr>
<tr>
<td>Admin</td>
<td>Admin &gt; Notification &gt; 00002</td>
</tr>
<tr>
<td>Auth</td>
<td>Auth &gt; Notification &gt; 00015</td>
</tr>
<tr>
<td>Clock</td>
<td>System &gt; Notification &gt; 00014</td>
</tr>
<tr>
<td>CLS</td>
<td>Notification &gt; 00043</td>
</tr>
<tr>
<td>CMS</td>
<td>Device &gt; Notification &gt; 00022</td>
</tr>
<tr>
<td>Console</td>
<td>Admin &gt; Notification &gt; 00003</td>
</tr>
<tr>
<td>DHCP CLI</td>
<td>DHCP &gt; Notification &gt; 00027</td>
</tr>
<tr>
<td>DHCP IP</td>
<td>DHCP &gt; Notification &gt; 00009</td>
</tr>
<tr>
<td>DHCP Opt</td>
<td>DHCP &gt; Notification &gt; 00024</td>
</tr>
<tr>
<td>DIP</td>
<td>DIP &gt; Notification &gt; 00021</td>
</tr>
<tr>
<td>DNS</td>
<td>DNS &gt; Notification &gt; 00004</td>
</tr>
<tr>
<td>DNS REP</td>
<td>DNS &gt; Notification &gt; 00029</td>
</tr>
<tr>
<td>Erase</td>
<td>System &gt; Notification &gt; 00023</td>
</tr>
<tr>
<td>Hostname</td>
<td>System &gt; Notification &gt; 00006</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface &gt; Notification &gt; 00009</td>
</tr>
<tr>
<td>MIP</td>
<td>MIP &gt; Notification &gt; 00021</td>
</tr>
<tr>
<td>NSRP</td>
<td>High Availability &gt; Notification &gt; 00007</td>
</tr>
<tr>
<td>OSPF</td>
<td>OSPF &gt; Notification &gt; 00038</td>
</tr>
<tr>
<td>PKI</td>
<td>PKI &gt; Notification &gt; 00002</td>
</tr>
<tr>
<td>Policy</td>
<td>Policies &gt; Notification &gt; 00018</td>
</tr>
<tr>
<td>PPP</td>
<td>HDLC &gt; Notification &gt; 00042</td>
</tr>
<tr>
<td>PPPoE</td>
<td>PPPoE &gt; Notification &gt; 00034</td>
</tr>
<tr>
<td>RIP</td>
<td>RIP &gt; Notification &gt; 00045</td>
</tr>
<tr>
<td>Route</td>
<td>Route &gt; Notification &gt; 00011</td>
</tr>
<tr>
<td>Route Map</td>
<td>Route &gt; Notification &gt; 00048</td>
</tr>
<tr>
<td>Schedule</td>
<td>Schedule &gt; Notification &gt; 00020</td>
</tr>
<tr>
<td>Service</td>
<td>Service &gt; Notification &gt; 00012</td>
</tr>
<tr>
<td>Set ARP</td>
<td>ARP &gt; Notification &gt; 00051</td>
</tr>
<tr>
<td>Shaper</td>
<td>Traffic Shaping &gt; Notification &gt; 00002</td>
</tr>
<tr>
<td>SIP ALG</td>
<td>Flow &gt; Notification &gt; 00047</td>
</tr>
<tr>
<td>SME</td>
<td>NSM &gt; Notification &gt; 00033</td>
</tr>
<tr>
<td>SNMP</td>
<td>SNMP &gt; Notification &gt; 00031</td>
</tr>
<tr>
<td>SW Key</td>
<td>Entitlement &gt; Notification &gt; 00036</td>
</tr>
<tr>
<td>SSH</td>
<td>SSHv2 &gt; Notification &gt; 00026</td>
</tr>
<tr>
<td>SSL</td>
<td>SSL &gt; Notification &gt; 00035</td>
</tr>
<tr>
<td>Syslog</td>
<td>Syslog and WebTrends &gt; Notification &gt; 00019</td>
</tr>
<tr>
<td>Track IP</td>
<td>High Availability &gt; Notification &gt; 00050</td>
</tr>
</tbody>
</table>
## Information Log Entries

The Information category contains the following subcategories:

### Table 84: Information Log Entries

<table>
<thead>
<tr>
<th>Configuration Log Entry Subcategories</th>
<th>ScreenOS Message ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL WEB Filtering &gt; Notification &gt; 00013</td>
<td></td>
</tr>
<tr>
<td>User User &gt; Notification &gt; 00014</td>
<td></td>
</tr>
<tr>
<td>VPN VPN &gt; Notification &gt; 00017</td>
<td></td>
</tr>
<tr>
<td>Vrouter Virtual Router &gt; Notification &gt; 00049</td>
<td></td>
</tr>
<tr>
<td>Vssys Vsys &gt; Notification &gt; 00032</td>
<td></td>
</tr>
<tr>
<td>Zone Zone &gt; Notification &gt; 00037</td>
<td></td>
</tr>
<tr>
<td>Set ARP Always On Dest ARP &gt; Notification &gt; 0005</td>
<td></td>
</tr>
<tr>
<td>Unset ARP Always On Dest ARP &gt; Notification &gt; 00054</td>
<td></td>
</tr>
</tbody>
</table>

**Information Log Entry Subcategories**

<table>
<thead>
<tr>
<th>Information Log Entry Subcategories</th>
<th>ScreenOS Message ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auth Challenge Auth &gt; Information &gt; 00546</td>
<td></td>
</tr>
<tr>
<td>Auth Failed Auth &gt; Warning &gt; 00518</td>
<td></td>
</tr>
<tr>
<td>Auth Status Change Auth &gt; Information &gt; 00525</td>
<td></td>
</tr>
<tr>
<td>Auth Passed Auth &gt; Warning &gt; 00519</td>
<td></td>
</tr>
<tr>
<td>Auth Timeout Auth &gt; Warning &gt; 00520</td>
<td></td>
</tr>
<tr>
<td>Anti Virus AntiVirus Scanning (External) &gt; Information &gt; 00547</td>
<td></td>
</tr>
<tr>
<td>BGP BGP &gt; Information &gt; 00542</td>
<td></td>
</tr>
<tr>
<td>Clock NTP &gt; Notification &gt; 00531</td>
<td></td>
</tr>
<tr>
<td>Configuration Size System &gt; Notification &gt; 00553</td>
<td></td>
</tr>
<tr>
<td>Device Connect N/A</td>
<td></td>
</tr>
<tr>
<td>Device Disconnect N/A</td>
<td></td>
</tr>
<tr>
<td>DHCP CLI DHCP &gt; Information &gt; 00530</td>
<td></td>
</tr>
<tr>
<td>DHCP DNS DNS &gt; Information &gt; 00004</td>
<td></td>
</tr>
<tr>
<td>Generic System &gt; Information &gt; 00767</td>
<td></td>
</tr>
<tr>
<td>VIP Svr Up VIP &gt; Notification &gt; 00533</td>
<td></td>
</tr>
<tr>
<td>Link Status Interface &gt; Notification &gt; 00513</td>
<td></td>
</tr>
<tr>
<td>Log Cleared Logging &gt; Information &gt; 00534</td>
<td></td>
</tr>
<tr>
<td>NSRD NSRD &gt; Information &gt; 00551</td>
<td></td>
</tr>
<tr>
<td>NTP failure NTP &gt; Notification &gt; 00531</td>
<td></td>
</tr>
<tr>
<td>NTP timeout NTP &gt; Notification &gt; 00531</td>
<td></td>
</tr>
<tr>
<td>OSPF OSPF &gt; Information &gt; 00541</td>
<td></td>
</tr>
<tr>
<td>Password Change Admin &gt; Information &gt; 00002</td>
<td></td>
</tr>
</tbody>
</table>
### Information Log Entry

<table>
<thead>
<tr>
<th>Subcategories</th>
<th>ScreenOS Message ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>PKI</td>
<td>PKI &gt; Information &gt; 00535</td>
</tr>
<tr>
<td>PPP</td>
<td>PPP &gt; Notification &gt; 00539</td>
</tr>
<tr>
<td>PPPoE</td>
<td>PPPoE &gt; Notification &gt; 00034</td>
</tr>
<tr>
<td>RIP</td>
<td>RIP &gt; Information &gt; 00544</td>
</tr>
<tr>
<td>SME</td>
<td>NSM &gt; Information &gt; 00538</td>
</tr>
<tr>
<td>SNMP</td>
<td>SNMP &gt; Information &gt; 00524</td>
</tr>
</tbody>
</table>
| SSH           | SSHv1 > Information > 00528  
 |               | SSHv2 > Information > 00026 |
| SSL           | SSL > Information > 00284 |
| URL Blk       | WEB Filtering > Notification > 00523 |
| Username Change | Admin > Information > 00002 |
| VPN           | VPN > Information > 00536  
 |               | L2TP > Information > 00536  
 |               | IKE > Information > 00536 |
| VIP Server Status | VIP > Notification > 00533 |
| DHCP Server Status | DHCP > Information > 00527 |

**NOTE:** For security devices running ScreenOS 5.0.x or higher, NetScreen-Security Manager does not generate information logs for device connect and disconnect events. The Realtime Monitor however, does display the correct up/down status of the device.

### Self Log Entries

Self log entries appear in the Log Viewer under the category Self, which contains a single subcategory: Self Log.

### Traffic Log Entries

Traffic log entries appear in the Log Viewer under the category Traffic, which contains a single subcategory: Traffic Log.

### GTP Log Entries

When you enable logging in a GTP object, you can configure a security device to create log entries with Basic or Extended information. Additionally, when counting is also enabled the GTP object, the device also generates log entries for deleted GTP tunnels.

For log entries generated by GTP objects with Basic logging enabled, you can view the following information:
Table 85: Basic GTP Log Entry

<table>
<thead>
<tr>
<th>Basic GTP Log Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timestamp</td>
</tr>
<tr>
<td>Source IP address</td>
</tr>
<tr>
<td>Destination IP address</td>
</tr>
<tr>
<td>TID (Tunnel Identifier)</td>
</tr>
<tr>
<td>TEID (Tunnel Endpoint Identifier)</td>
</tr>
<tr>
<td>Message type</td>
</tr>
<tr>
<td>Packet status: forwarded, prohibited, state-invalid, rate-limited, or tunnel-limited</td>
</tr>
<tr>
<td>Interface, vsys, or vrouter name (if applicable)</td>
</tr>
<tr>
<td>PLMN or zone name</td>
</tr>
</tbody>
</table>

For log entries generated by GTP objects with Extended logging enabled, you can view the following information:

Table 86: Extended GTP Log Entry

<table>
<thead>
<tr>
<th>Extended GTP Log Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>IMSI</td>
</tr>
<tr>
<td>MSISDN</td>
</tr>
<tr>
<td>APN</td>
</tr>
<tr>
<td>Selection Mode</td>
</tr>
<tr>
<td>SGSN address for signaling</td>
</tr>
<tr>
<td>SGSN address for user data</td>
</tr>
<tr>
<td>GGSN address for signaling</td>
</tr>
<tr>
<td>GGSN address for user data</td>
</tr>
</tbody>
</table>

For log entries generated by deleted GTP tunnels, you can view the following information:

Table 87: Deleted GTP Tunnel Log Entry

<table>
<thead>
<tr>
<th>Deleted GTP Tunnel Log Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timestamp</td>
</tr>
<tr>
<td>Interface name (if applicable)</td>
</tr>
<tr>
<td>SGSN IP address</td>
</tr>
<tr>
<td>GGSN IP address</td>
</tr>
<tr>
<td>TID</td>
</tr>
<tr>
<td>Tunnel duration time in seconds</td>
</tr>
<tr>
<td>Number of messages sent to the SGSN</td>
</tr>
<tr>
<td>Number of messages sent to the GGSN</td>
</tr>
</tbody>
</table>
Appendix E
Common Criteria EAL2 Compliance

This appendix describes actions required for a security administrator to properly secure the NetScreen-Security Manager system and NetScreen-Security Manager User Interface to be in compliance with the Common Criteria EAL2 security target for Juniper Networks IDP 3.0 functionality.

The NetScreen-Security Manager system consists of the Device Server and the Gui Server; the NetScreen-Security Manager User Interface is a client application used to access information stored in the NetScreen-Security Manager system.

Guidance for Intended Usage

- The NetScreen-Security Manager system must be installed on dedicated systems. These dedicated systems must not contain user processes that are not required to operate the NetScreen-Security Manager software.

Guidance for Personnel

- There must be one or more competent individuals assigned to manage the NetScreen-Security Manager system and User Interface, and the security of the information that they contain.

- The authorized administrators must not be careless, willfully negligent, or hostile and must follow and abide by the instructions provided by the NetScreen-Security Manager documentation.

- The NetScreen-Security Manager system and User Interface must be accessed only by authorized users.

Guidance for Physical Protection

- The processing resources of the NetScreen-Security Manager system and User Interface must be located within facilities with controlled access which prevents unauthorized physical access.
The Index in Part 6 of the NetScreen-Security Manager 2005.3 Administrators Guide provides an alphabetical listing of important terms and concepts used in this guide, as well as the page numbers on which those terms and concepts are found.
**Index**

Numerics
802.11b support........................................................... 156
802.11g support........................................................... 156

A
Abstract Data Model .................................................. 432
access lists
configuring............................................................. 172
defined............................................................... 803
access lists on WAP.................................................. 159
Access Point Name
See APN
access-challenge, defined........................................... 803
ACLs on WAP.......................................................... 159
actions, configuring in firewall rules............................ 541
active sessions
information available..................................................... 703–704
session display filter..................................................... 705
session filter............................................................. 704
viewing................................................................. 703–705
active statistics
about...................................................................... 690
viewing................................................................... 703
active VPN
details, viewing.......................................................... 708
information, viewing..................................................... 696
activities
admin roles............................................................... 60
admins...................................................................... 60
attack update............................................................. 60
audit logs................................................................. 60
device certificates....................................................... 61
device configuration.................................................... 61
device delta config...................................................... 61
device firmware........................................................ 61
device log comments................................................... 61
device log flags............................................................ 61
device logs............................................................... 61
device passwords......................................................... 61
device reboot.............................................................. 61
device running config.................................................. 62
device software keys.................................................... 62
device status monitor................................................... 62
device URL categories.................................................. 62
devices, groups, templates........................................... 62
firewall rulebases......................................................... 62
HA for guiSvClusterMgr............................................... 62
historical reports......................................................... 62
investigative log reports............................................... 62
jobs........................................................................ 63
multicast rulebases....................................................... 63
NSRP Monitor............................................................. 63
policy lookup table...................................................... 63
rulebases.................................................................. 63
security policies.......................................................... 63
servers..................................................................... 63
shared objects and groups.......................................... 63
subdomains and groups.............................................. 63
system URL categories................................................. 64
VPN Monitor............................................................... 64
VPNs....................................................................... 64
address objects
about..................................................................... 444
configuring in firewall rules...................................... 537
defined.................................................................... 803
address shifting
defined.................................................................... 803
See NAT-dst and NAT-src
address spoofing, defined.......................................... 803
adjacencies, defined................................................... 803
administrative reports................................................ 782, 785, 795
administrators
creating................................................................... 57
permissions................................................................ 60
ADSL
configuring backup link on device............................... 263
configuring interface................................................... 260
connecting the cable................................................... 261
ISP settings............................................................... 261
LLC multiplexing......................................................... 261
multiplexing mode....................................................... 261
operating mode (DMT)................................................ 262
operating mode, ANSI T1.413 Issue 2.......................... 262
operating mode, ITU 992.2 (G.lite)................................ 262
operating mode, ITU G 992.1...................................... 262
supported port modes................................................. 262
VC multiplexing......................................................... 261
VPI/VCI settings......................................................... 261
advanced device options............................................. 330
advanced network settings
ARP cache.................................................................. 295
DIP options................................................................ 295
VIP options................................................................ 295
advertisement, defined.............................................. 804
AES
about..................................................................... 165
defined.................................................................... 803
ageing, configuring on device...................................... 342
aggregate interface....................................................... 250
aggregate state, defined.............................................. 804
aggregation, defined................................................... 804
aggregator, defined..................................................... 804
aggressive aging, defined.......................................... 804
aging settings on WAP................................................. 157
alarms, configuring in firewall rules.............................. 545
alerts, configuring in firewall rules................................ 545
ALG
configuring on device................................................ 335
profiles ..........................................................317
Scan Manager .................................................317
scanning, defined ..............................................804
update pattern file .............................................426

B
backdoor rulebase
about ..............................................................572
adding to Security Policy .................................573
backdoor rules
configuring ......................................................572–576
configuring actions ...........................................574
configuring Match columns ...............................573
configuring notification ......................................575
configuring operation ........................................574
configuring services .........................................574
configuring severity ..........................................576
configuring source and destination .......................574
counting targets ...............................................576
configuring zones .............................................574
entering comments ...........................................576
backup interface, fail over ..................................429
backup link for adsl interface ..............................263
banners, configuring on device .............................311
basic service sets on WAP ................................160
bastion host, defined .........................................805
beacon settings on WAP .....................................157
BGP
about ..............................................................198
configuring aggregate addresses .........................200
configuring neighbors and peer groups .................200
configuring networks ........................................199
configuring on device .......................................198
configuring route maps ....................................200
defined ............................................................805
keepalive, defined ...........................................811
neighbor, defined ............................................805
peer connection troubleshooting ..........................430
route attributes ...............................................199
broadcast networks, defined ..............................806
BSS ..............................................................160
BugTraq references ...........................................459
burst settings on WAP .......................................157

C
CA certificates, configuring on device ....................371
certificate authorities .......................................517
certificates
certificate request ..........................................367
configuring on device .......................................366
CRLs ..............................................................372
generating request ...........................................367
imported certificates ........................................373
installing certificates .......................................369
local certificates .............................................367
PKI defaults ....................................................373
revocation settings .........................................374
SCEP .............................................................370, 371, 375
viewing CA certificates ....................................371
X509 certificates ................................................373
changes that affect device connection ..................132
channel settings on WAP ..................................155
chart type, configuring .....................................792
CIDR, defined .................................................806
Classless Inter-Domain Routing, defined ...............806
classless routing, defined .................................806
CLI banners, configuring on device ......................306
CLI commands, displaying ...............................431
CLI management .............................................302
CLI, defined ....................................................806
cluster
See SRSP cluster
cluster list for BGP, defined ...............................806
community for BGP, defined ...............................806
compound attack objects
custom ..........................................................471
custom, adding protocol anomaly .......................473
custom, configuring attack pattern ......................473
custom, configuring ordered match ......................473
custom, configuring scope ................................472
configuration for BGP, defined .........................806
configlet, defined ............................................806
configuration logs report ....................................784
configuration states ..........................................396
configuration summary, running .........................400, 404
configuring
devices ..........................................................129–388
logging ............................................................719–780
monitoring .......................................................681–717
objects ............................................................441–525
reporting .........................................................781–800
role-based administration ..................................51–70
security policies ..............................................527–590
VPNs ............................................................591–678
configuring in rule .............................................553
connection attempts, max ..................................303
connection states .............................................396
connections, BGP peer .....................................430
console-only restrictions ....................................304
control frame protection settings on WAP .............158
counting, configuring in firewall rules ...................545
CRLs (certificate protection list) ..........................520
CTS/RTS settings .............................................158
customer support ............................................xliii
CVE references ...............................................458

D
Data Model
defined ..........................................................432
importing .........................................................435
schema ..........................................................433
updating ..........................................................433
data model, defined ........................................807
data point count ..............................................758, 792
data rate settings on WAP ................................156
data types .......................................................758
Deep Inspection
activating subscription on device .........................415
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>attack objects, custom</td>
<td>456</td>
</tr>
<tr>
<td>checking attack object database</td>
<td>419</td>
</tr>
<tr>
<td>configuring on device</td>
<td>326</td>
</tr>
<tr>
<td>local attack object update</td>
<td>416</td>
</tr>
<tr>
<td>profiles in firewall rules</td>
<td>551</td>
</tr>
<tr>
<td>profiles, about</td>
<td>449</td>
</tr>
<tr>
<td>updating attack object database</td>
<td>415</td>
</tr>
<tr>
<td>default values in templates</td>
<td>135</td>
</tr>
<tr>
<td>delta configuration summary</td>
<td>400</td>
</tr>
<tr>
<td>demand circuit, configuring for tunnel interface</td>
<td>191</td>
</tr>
<tr>
<td>deny action, configuring in firewall rules</td>
<td>541</td>
</tr>
<tr>
<td>dependant activities</td>
<td>60</td>
</tr>
<tr>
<td>DES, defined</td>
<td>807</td>
</tr>
<tr>
<td>DES-CBC, defined</td>
<td>807</td>
</tr>
<tr>
<td>destination NAT, configuring in firewall rules</td>
<td>543</td>
</tr>
<tr>
<td>destination routing table</td>
<td>180</td>
</tr>
<tr>
<td>device administration</td>
<td></td>
</tr>
<tr>
<td>about</td>
<td>296</td>
</tr>
<tr>
<td>CLI management</td>
<td>302</td>
</tr>
<tr>
<td>CLI management, asset recovery</td>
<td>303</td>
</tr>
<tr>
<td>CLI management, CLI banners</td>
<td>306</td>
</tr>
<tr>
<td>CLI management, configuring SSH</td>
<td>304</td>
</tr>
<tr>
<td>CLI management, console-only restrictions</td>
<td>304</td>
</tr>
<tr>
<td>CLI management, file format</td>
<td>302</td>
</tr>
<tr>
<td>CLI management, max connection attempts</td>
<td>303</td>
</tr>
<tr>
<td>CLI management, reset hardware (device)</td>
<td>303</td>
</tr>
<tr>
<td>CLI management, restricting password length</td>
<td>303</td>
</tr>
<tr>
<td>CLI management, SSL and Telnet ports</td>
<td>302</td>
</tr>
<tr>
<td>configuring HTTP</td>
<td>307</td>
</tr>
<tr>
<td>configuring SSL</td>
<td>307</td>
</tr>
<tr>
<td>date/time</td>
<td>308</td>
</tr>
<tr>
<td>device admins, authentication method</td>
<td>300</td>
</tr>
<tr>
<td>device admins, passwords</td>
<td>300</td>
</tr>
<tr>
<td>device admins, privilege levels</td>
<td>298</td>
</tr>
<tr>
<td>device admins, public key authentication (PKA)</td>
<td>300</td>
</tr>
<tr>
<td>device admins, root</td>
<td>298</td>
</tr>
<tr>
<td>disabling SSL on device</td>
<td>308</td>
</tr>
<tr>
<td>permitted IPs</td>
<td>301</td>
</tr>
<tr>
<td>secondary banner</td>
<td>306</td>
</tr>
<tr>
<td>Web management</td>
<td>306</td>
</tr>
<tr>
<td>device administrator</td>
<td></td>
</tr>
<tr>
<td>configuring root</td>
<td>298</td>
</tr>
<tr>
<td>defined</td>
<td>807</td>
</tr>
<tr>
<td>device advanced settings</td>
<td></td>
</tr>
<tr>
<td>about</td>
<td>330</td>
</tr>
<tr>
<td>host and domain name</td>
<td>344</td>
</tr>
<tr>
<td>packet flow</td>
<td>336</td>
</tr>
<tr>
<td>predefined service timeouts</td>
<td>331</td>
</tr>
<tr>
<td>TFTP/FTP server</td>
<td>343</td>
</tr>
<tr>
<td>traffic shaping</td>
<td>334</td>
</tr>
<tr>
<td>device capabilities</td>
<td></td>
</tr>
<tr>
<td>file</td>
<td>433</td>
</tr>
<tr>
<td>viewing</td>
<td>151</td>
</tr>
<tr>
<td>device certificate options</td>
<td></td>
</tr>
<tr>
<td>about</td>
<td>366</td>
</tr>
<tr>
<td>CA certificates</td>
<td>371</td>
</tr>
<tr>
<td>certificate request</td>
<td>367</td>
</tr>
<tr>
<td>CRLs</td>
<td>372</td>
</tr>
<tr>
<td>imported certificates</td>
<td>373</td>
</tr>
<tr>
<td>local certificates</td>
<td>367</td>
</tr>
<tr>
<td>PKI defaults</td>
<td>373</td>
</tr>
<tr>
<td>SCEP</td>
<td>370, 371, 375</td>
</tr>
<tr>
<td>X509 certificates</td>
<td>373</td>
</tr>
<tr>
<td>device certificates, permissions</td>
<td>61</td>
</tr>
<tr>
<td>device clock, updating</td>
<td>428</td>
</tr>
<tr>
<td>device configuration</td>
<td></td>
</tr>
<tr>
<td>about</td>
<td>130</td>
</tr>
<tr>
<td>link from Log Viewer</td>
<td>752</td>
</tr>
<tr>
<td>memory optimization</td>
<td>130</td>
</tr>
<tr>
<td>permissions</td>
<td>61, 62</td>
</tr>
<tr>
<td>unsupported in UI</td>
<td>132</td>
</tr>
<tr>
<td>updating</td>
<td>403</td>
</tr>
<tr>
<td>device connection to Security Manager</td>
<td>132</td>
</tr>
<tr>
<td>device delta config, permission to view</td>
<td>61</td>
</tr>
<tr>
<td>device firmware</td>
<td></td>
</tr>
<tr>
<td>adjusting version</td>
<td>413</td>
</tr>
<tr>
<td>permission to update</td>
<td>61</td>
</tr>
<tr>
<td>device groups</td>
<td></td>
</tr>
<tr>
<td>permissions</td>
<td>62, 63</td>
</tr>
<tr>
<td>planning for</td>
<td>47</td>
</tr>
<tr>
<td>using</td>
<td>148</td>
</tr>
<tr>
<td>device interface settings</td>
<td></td>
</tr>
<tr>
<td>DHCP</td>
<td>226</td>
</tr>
<tr>
<td>DIPs</td>
<td>237</td>
</tr>
<tr>
<td>GRE</td>
<td>230</td>
</tr>
<tr>
<td>MIPs</td>
<td>230</td>
</tr>
<tr>
<td>NAT</td>
<td>230</td>
</tr>
<tr>
<td>secondary IP</td>
<td>229</td>
</tr>
<tr>
<td>VIPs</td>
<td>233</td>
</tr>
<tr>
<td>device log comments, permission to update</td>
<td>61</td>
</tr>
<tr>
<td>device log flags, permission to update</td>
<td>61</td>
</tr>
<tr>
<td>device logs, permissions</td>
<td>61</td>
</tr>
<tr>
<td>Device Manager module</td>
<td>18, 129</td>
</tr>
<tr>
<td>device monitor, defined</td>
<td>807</td>
</tr>
<tr>
<td>device network settings</td>
<td></td>
</tr>
<tr>
<td>dynamic routing protocols</td>
<td>185</td>
</tr>
<tr>
<td>virtual routers</td>
<td>169</td>
</tr>
<tr>
<td>device NSRP options</td>
<td></td>
</tr>
<tr>
<td>about</td>
<td>376</td>
</tr>
<tr>
<td>active/active</td>
<td>381</td>
</tr>
<tr>
<td>master/backup</td>
<td>383</td>
</tr>
<tr>
<td>synchronizing</td>
<td>382</td>
</tr>
<tr>
<td>device passwords, permission to view</td>
<td>61</td>
</tr>
<tr>
<td>device policy pointers</td>
<td>587</td>
</tr>
<tr>
<td>device reboot, permission</td>
<td>61</td>
</tr>
<tr>
<td>device references, finding</td>
<td>431</td>
</tr>
<tr>
<td>device reporting options</td>
<td></td>
</tr>
<tr>
<td>email notification</td>
<td>313</td>
</tr>
<tr>
<td>general</td>
<td>313</td>
</tr>
<tr>
<td>NSM</td>
<td>314</td>
</tr>
<tr>
<td>SNMP</td>
<td>314</td>
</tr>
<tr>
<td>syslog</td>
<td>314</td>
</tr>
<tr>
<td>WebTrends</td>
<td>315</td>
</tr>
<tr>
<td>device running config, permission to view</td>
<td>62</td>
</tr>
<tr>
<td>device security module</td>
<td></td>
</tr>
<tr>
<td>See security module</td>
<td></td>
</tr>
<tr>
<td>device security options</td>
<td></td>
</tr>
<tr>
<td>about</td>
<td>315</td>
</tr>
<tr>
<td>antivirus</td>
<td>315</td>
</tr>
<tr>
<td>attack database</td>
<td>327</td>
</tr>
</tbody>
</table>
Index

Deep Inspection .................................................. 326
disabling attack objects ........................................... 328
URL filtering ........................................................ 322
Device Server
about ................................................................. 13
defined .................................................................. 807
permissions .......................................................... 63
processes .............................................................. 14
device software keys, permission to install ............... 62
device status ......................................................... 396
device status monitor, permission to view ................. 62
device templates .................................................. 47
See also templates
device traffic distribution, viewing ......................... 690
device update, errors ............................................ 409
device vsys options
about ..................................................................... 351
interfaces ............................................................... 353
virtual routers ...................................................... 352
zones .................................................................... 353
devices, configuring in firewall rules ......................... 541
devices, re-importing ............................................. 586
device-specific VPN information, viewing ............... 708
DHCP
configuring in device ............................................ 226
custom DHCP options .......................................... 227
defined .................................................................. 807
DI
See Deep Inspection
DI profiles
creating .................................................................. 451
DI reports ........................................................... 782, 784
dial backup
configuring for route-based VPN member ............... 616
enabling in VPN Manager .................................. 612
Diffie-Hellman Group ........................................... 523
DIP groups, configuring ....................................... 273
DIP options, configuring on device ......................... 295
DIP translation stickiness ........................................ 296
DIPs
configuring in device ............................................ 237
extended interface ................................................. 238
global objects ...................................................... 516
incoming DIP for SIP ........................................... 244
port translation ...................................................... 237
directive
defined .................................................................. 807
tracking with Job Manager .................................. 406
discrete multitone .................................................. 262
display filter ........................................................... 708
diversity antennas ................................................. 154
DMT ................................................................. 262
DMZ, defined ....................................................... 807
DNS
configuring on device .......................................... 289
defined .................................................................. 807
dynamic DNS, configuring on device ....................... 292
proxy, configuring on device .................................. 289
refreshing entries .................................................. 427
DNS reply without matched request, allow ............. 337
domain name, configuring on device ....................... 344
domains
about ................................................................... 52
defined .................................................................. 808
global domain login ............................................. 59
setting a Log Viewer filter for ..................... 746
versioning ........................................................... 65
viewing domain details ........................................ 65
DSCP class selector .............................................. 335, 544
DSL ................................................................. 280
dynamic DNS ....................................................... 292
dynamic host configuration protocol
See DHCP
dynamic IP pools
See DIPs
dynamic routing protocols
about ................................................................. 185
BGP ................................................................. 198
defined .................................................................. 808
OSPF ............................................................... 186
RIP ................................................................. 193
E
ECMP routes, configuring maximum on virtual router 171
e-mail notification, configuring on device ............... 313
encrypting NSRP traffic ....................................... 377
encryption, defined ............................................. 808
tenentishment
See subscription
ESP/AH, defined .................................................. 808
ethernet statistics
device-specific view, described ............................ 690
viewing ............................................................... 697–698
ethernet statistics, viewing .................................... 697–698
ethernet, defined .................................................. 808
exempt rulebase
about ................................................................... 569
adding to Security Policy .................................... 569
exempt rules
configuring ........................................................ 569–572
configuring attacks .............................................. 570
configuring from the Log Viewer ................... 571
configuring match columns ................................ 569
configuring source and destination ..................... 570
configuring targets .............................................. 571
configuring zones ............................................... 570
entering comments ............................................. 571
expanded VPN view ............................................ 592, 627
export rules
configuring on virtual router ............................... 175
defined ............................................................. 808
exporting log entries
from device to email ............................................. 726
from device to NSM ............................................ 726
from device to SNMP .......................................... 732
from device to syslog .......................................... 733
from device to WebTrends ................................. 734
from device, about ............................................. 724
from device, self log entries ............................... 725

Index  ■  911
from GUI Server to CSV ........................................ 771
from GUI Server to email...................................... 771
from GUI Server to script .................................... 772
from GUI Server to SNMP .................................... 770
from GUI Server to syslog ................................... 770
from GUI Server to XML ...................................... 771
from GUI Server, about ...................................... 769
from log2action to CSV ....................................... 775
from log2action to email ...................................... 777
from log2action to script .................................... 779
from log2action to SNMP .................................... 776
from log2action to syslog .................................... 778
from log2action to XML ...................................... 775
exporting Log Viewer views ................................ 751
exporting security policies ................................... 589
extended information for custom attack object .......... 458
extended port mode ............................................. 91, 94, 98
external AV scanner
  about ............................................................. 316
  fail mode traffic permit ...................................... 316
  HTTP keep-alive ............................................. 316
  skip scanning HTTP ........................................ 316
  trickling ....................................................... 317
external neighbors for BGP, defined ..................... 808
external references for custom attack object .......... 458
external user groups ......................................... 508
external users .................................................. 806
extranet, defined .............................................. 808
configuring antivirus ......................................... 551
configuring application relocation ......................... 547
configuring authentication ................................... 550
configuring counting and alarms ......................... 545
configuring devices ......................................... 541
configuring DI profile ....................................... 551
configuring GTP object ....................................... 543
configuring HA session backup ............................. 547
configuring logging and counting ......................... 545
configuring NAT .............................................. 542
configuring preferred ID ..................................... 547
configuring rule options .................................... 542
configuring rule title ........................................ 553
configuring scan manager ................................... 551
configuring schedule ......................................... 546
configuring services ......................................... 540
configuring traffic shaping ................................... 543
configuring URL filtering profile ......................... 548
configuring zones ............................................. 537
deleting ......................................................... 585
deny action ...................................................... 541
disabling ......................................................... 585
negating source or destination .............................. 538
permit action ................................................... 541
reject action .................................................... 541
reject action changed to deny ............................... 579
rule groups ...................................................... 585
using MIPs as source or destination ...................... 538
VPN links ....................................................... 531
VPN rules ....................................................... 531
zone exceptions .............................................. 583
firewall definition ........................................... 130
firewall, definition ........................................... 130
firmware, adjusting version on device ................... 413
first packet context for custom attack object .......... 466
flag ................................................................. 774
flow initial session timeout ................................ 341
flow properties, viewing ..................................... 466
flow statistics
  device-specific view, described ......................... 690
  viewing ....................................................... 699
forcing device mode in NSRP cluster ...................... 376
FQDN ............................................................. 622
fragment reassembly .......................................... 213–222
fragmentation settings on WAP ............................. 158
fragmented packet size, maximum ......................... 341
FTP banner ...................................................... 311
FTP server, configuring on device ......................... 344
FW/VPN reports ............................................... 782, 784
G
G.lite ............................................................... 262
gateway router, defined ..................................... 809
gateway tracking ............................................... 181
GBIC, defined .................................................. 809
GGSN, defined .................................................. 809
Gt interface, defined .......................................... 809
GMT, defined ................................................... 809
Gn interface, defined .......................................... 809
Gp interface, defined .......................................... 809

F
failover
  configuring on interface ................................... 286
  forcing on device interface ................................. 429
false positive setting ........................................ 460
filtering logs using ranges ................................ 747
filters
  negation ......................................................... 745
  setting a byte range filter ................................ 747
  setting a category filter ................................... 745
  setting a domain filter ..................................... 746
  setting a flag filter ........................................ 746
  setting a port range filter ................................ 748
  setting a protocol filter .................................. 747
  setting a range filter ....................................... 747
  setting a time-based filter ................................ 746
  setting an address filter ................................... 746
  setting an alert filter ...................................... 745
find utility ....................................................... 744
firewall options ............................................... 725
firewall rulebase
  about ............................................................. 530
  permissions ................................................... 62
  rule groups .................................................... 531
firewall rules
  about ............................................................. 530
  configuring ..................................................... 536–553
  configuring actions ........................................... 541
  configuring address objects ................................ 537
  configuring alerts ............................................. 545

912  ■  Index
configuring on device .......................................................... 286
forcing on device ................................................................ 429
interface statistics, viewing .................................................. 697
interfaces
ADS ................................................................. 260
advanced properties .................................................... 225
aggregate ........................................................................ 250
configuring for vsys ...................................................... 353
configuring on device .................................................... 222
configuring WebAuth ..................................................... 225
device-specific views, described ........................................ 690
elements ........................................................................... 250
genral properties ............................................................. 224
loopback ........................................................................... 251
protocol, configuring .................................................... 229
redundant .......................................................................... 253
service options ................................................................. 226
statistics ........................................................................... 697
subinterface ....................................................................... 257
tunnel ................................................................................. 258
tunnel, defined ............................................................... 820
tunnel, MTU size .............................................................. 260
virtual security (VSI) ........................................................ 252
internal AV scanner
content drop parameters ................................................. 317
content protocol ................................................................. 317
pattern server URL ........................................................... 317
update interval ................................................................. 317
Internet Group Management Protocol
See IGMP
intrusion detection and prevention
See IDP
investigative log reports, permissions ............................... 62
IP address, defined .......................................................... 811
IP gateway, defined ......................................................... 811
IP header matches for custom attack object ...................... 467
IP pools
configuring ................................................................. 511
defined ........................................................................... 811
using multiple ranges ....................................................... 511
IP tracking, defined .......................................................... 811
IP, defined ........................................................................ 811
IPSec, defined ................................................................. 811
ISAKMP, defined .............................................................. 811
ISP settings, configuring on device ..................................... 288
ITU 992.2 ................................................................. 262
ITU G.992.1 ................................................................... 262
J
Job Manager
about ............................................................................. 21
defined ........................................................................... 811
job status logs, permission to purge ................................. 62
jobs, permission to view ................................................... 63
K
key list parameters in templates ........................................ 136
L
L2TP
configuring in device-level VPNS ........................................ 662
configuring in VPN Manager ............................................. 614
lawful interception in GTP object ........................................ 490
left axis, Log Investigator .................................................. 757
license key
displaying for device ....................................................... 414
installing on device ........................................................ 414
obtaining ................................................................. 414
line context for custom attack object .................................. 466
link state advertisement, defined ..................................... 812
link state, defined ............................................................ 812
linking to a device from Log Viewer ................................ 752
load balancing, defined .................................................... 812
local attack object update ................................................ 416
local preference for BGP, defined ..................................... 812
local user groups ............................................................. 507
local users ........................................................................ 606
log actions
about ............................................................................. 770
csv ............................................................................... 771
e-mail .......................................................................... 771
SNMP ........................................................................... 770
syslog .......................................................................... 770
xml ............................................................................ 771
log categories
defined ........................................................................... 812
filtering in Log Viewer .................................................... 745
log criteria ........................................................................ 772
log destinations
configuring on device ..................................................... 313
email server .................................................................... 726
Syslog ........................................................................... 733
WebTrends server ............................................................ 734
log entries
actions ............................................................................. 770
criteria ........................................................................... 770
enabling in firewall rules ................................................ 545
exporting ........................................................................ 770
filtering with ranges ....................................................... 747
identifying patterns .......................................................... 398
searching by ID ................................................................. 744
severity levels ................................................................. 722
SNMP ........................................................................... 732
using the Find utility ........................................................ 744
log ID, defined ................................................................. 812
Log Investigator
about ............................................................................. 18
configuring axes ............................................................. 757
defined ........................................................................... 812
setting data point count .................................................. 758
setting data types ........................................................... 758
log severity
alert ................................................................................. 722
configuring on device ..................................................... 313
critical .................................................................... 722
debugging ................................................................. 724
emergency ................................................................. 722
error .......................................................... 722
information .................................................. 723
levels .......................................................... 722
notification .................................................. 723
warning ...................................................... 722
log sub-categories ........................................ 745
log types
  config ...................................................... 721
  custom .................................................... 721
  info ........................................................ 721
  predefined .............................................. 721
  screen ..................................................... 721
  self ......................................................... 721
  traffic ..................................................... 721
Log Viewer
  about ........................................................ 18
  creating an exempt rule ................................ 571
  defined ...................................................... 812
  exporting views ........................................ 751
  filtering ................................................... 744
  find utility ................................................ 744
  flags ......................................................... 743
  integration with reports ................................ 793
  linking to a device ..................................... 752
  log categories .......................................... 745
  log ID ...................................................... 744
  log sub-categories ...................................... 745
  saving a view ............................................ 751
  saving custom views ................................... 751
  unknown values ........................................ 739
  using ranges for filtering ................................ 747
  view ........................................................ 751
log, defined .................................................. 812
log2action
  common options ........................................ 773
  exporting to CSV ........................................ 775
  exporting to script ...................................... 779
  exporting to SMTP (email) ............................ 777
  exporting to SNMP ...................................... 776
  exporting to syslog ...................................... 778
  exporting to XML .................................... 775
logging
  configuring in firewall rules ......................... 545
  self log entries ........................................ 725
Logs by User-set Flag report ............................. 786, 796
loopback interface
  configuring ............................................... 251
  defined ...................................................... 812
M
MAC access lists on WAP ................................ 159
MAC flooding, allow unknown .......................... 338
main display area ........................................... 17
malicious URL protection .................................. 220–222
manage IP VSD group 0 .................................... 377
managed devices ............................................. 14
management options for device administrators
  SSH ......................................................... 226
  Telnet ...................................................... 226
WebUI .......................................................... 226
manual key ................................................... 666
mapped IPs
  See MIPs
MCC, defined .................................................. 813
MD5, defined .................................................. 813
Media Gateway Control Protocol, defined ............ 813
member AS, defined ....................................... 813
merging security policies .................................. 586
meshing, disabling in VPN Manager ..................... 617
messages
  configuring logging on device ....................... 313
  email notification for device ....................... 313
  metric, defined ................................. 813
  MIB II .................................................... 226
Microsoft Remote Procedure Call (MS-RPC) ........... 493
MIPs
  configuring in device ................................ 230
  defined ..................................................... 813
  global objects ......................................... 517
  using in rules ......................................... 538
  MNC, defined ........................................... 813
  Mobile Country Code (MCC) ...................... 490
  Mobile Network Code (MNC) .................. 490
  Mobile Subscriber Identification Number (MSIN) .... 490
  modem, extended port ................................ 91, 94, 98
  modeling, defined .................................. 813
  modem connection configuration .................... 287
  modem settings, configuring on device .............. 287
  module, defined ........................................ 813
  modules, NetScreen-Security Manager .............. 17
  monitoring
    NSRP statistics ...................................... 708
    VPN Status ........................................ 706
  MS, defined ......................................... 813
  MSIN, defined ........................................ 813
multicast routing
  about ..................................................... 201
  IGMP .................................................... 202
  IGMP proxy ............................................ 203
  negative mroute cache ................................ 210
  PIM-DM ................................................ 203
  PIM-SM ................................................ 209
  routing table entries ................................ 209
multicast rulebase
  about ..................................................... 532
  permissions ............................................... 63
multicast rules
  configuring ............................................. 553–555
  deleting .................................................. 585
  disabling ................................................ 585
N
NACN, configuring on device ............................... 286
NAT objects
  about ..................................................... 516
  configuring in firewall rules ......................... 542
  DIP, global ............................................. 516
  in VPNs .................................................. 605
  MIP, global ............................................. 517
Index
Microsoft Remote Procedure Call (MS-RPC) ........... 493
MIPs
  configuring in device ................................ 230
  defined ..................................................... 813
  global objects ......................................... 517
  using in rules ......................................... 538
  MNC, defined ........................................... 813
  Mobile Country Code (MCC) ...................... 490
  Mobile Network Code (MNC) .................. 490
  Mobile Subscriber Identification Number (MSIN) .... 490
  modem, extended port ................................ 91, 94, 98
  modeling, defined .................................. 813
  modem connection configuration .................... 287
  modem settings, configuring on device .............. 287
  module, defined ........................................ 813
  modules, NetScreen-Security Manager .............. 17
  monitoring
    NSRP statistics ...................................... 708
    VPN Status ........................................ 706
  MS, defined ......................................... 813
  MSIN, defined ........................................ 813
multicast routing
  about ..................................................... 201
  IGMP .................................................... 202
  IGMP proxy ............................................ 203
  negative mroute cache ................................ 210
  PIM-DM ................................................ 203
  PIM-SM ................................................ 209
  routing table entries ................................ 209
multicast rulebase
  about ..................................................... 532
  permissions ............................................... 63
multicast rules
  configuring ............................................. 553–555
  deleting .................................................. 585
  disabling ................................................ 585
N
NACN, configuring on device ............................... 286
NAT objects
  about ..................................................... 516
  configuring in firewall rules ......................... 542
  DIP, global ............................................. 516
  in VPNs .................................................. 605
  MIP, global ............................................. 517
Index
Microsoft Remote Procedure Call (MS-RPC) ........... 493
MIPs
  configuring in device ................................ 230
  defined ..................................................... 813
  global objects ......................................... 517
  using in rules ......................................... 538
  MNC, defined ........................................... 813
  Mobile Country Code (MCC) ...................... 490
  Mobile Network Code (MNC) .................. 490
  Mobile Subscriber Identification Number (MSIN) .... 490
  modem, extended port ................................ 91, 94, 98
  modeling, defined .................................. 813
  modem connection configuration .................... 287
  modem settings, configuring on device .............. 287
  module, defined ........................................ 813
  modules, NetScreen-Security Manager .............. 17
  monitoring
    NSRP statistics ...................................... 708
    VPN Status ........................................ 706
  MS, defined ......................................... 813
  MSIN, defined ........................................ 813
multicast routing
  about ..................................................... 201
  IGMP .................................................... 202
  IGMP proxy ............................................ 203
  negative mroute cache ................................ 210
  PIM-DM ................................................ 203
  PIM-SM ................................................ 209
  routing table entries ................................ 209
multicast rulebase
  about ..................................................... 532
  permissions ............................................... 63
multicast rules
  configuring ............................................. 553–555
  deleting .................................................. 585
  disabling ................................................ 585
N
NACN, configuring on device ............................... 286
NAT objects
  about ..................................................... 516
  configuring in firewall rules ......................... 542
  DIP, global ............................................. 516
  in VPNs .................................................. 605
  MIP, global ............................................. 517
Index

NetScreen-Security Manager 2005.3 Administrator's Guide

Index

VIP, global .......................................................... 517
NAT Traversal ......................................................... 619
NAT, configuring on device .................................. 230
navigation tree ...................................................... 17
negating source or destination in firewall rules ........ 538
negative mrout cache .............................................. 210
neighbor for BGP, defined .................................... 813
NetScreen Address Change Notification
See NACN
NetScreen dictionary file ..................................... 502
NetScreen Gatekeeper Protocol
See NSGP
NetScreen Redundancy Protocol
See NSRP
NetScreen-IGS 2000 security system ........................ 131
NetScreen-Security Manager modules .................. 17
network address translation
See NAT
network modules
about ................................................................. 167
card slots .......................................................... 169
copper I/O cards .................................................. 167
fiber I/O cards ..................................................... 168
secure port modules (SPM) ..................................... 168
network options, configuring on device ............... 152
Network Time Protocol (NTP) ............................... 308
next-hop, configuring on virtual router .................. 172
NHTB, configuring in VPN Manager ..................... 616
NSAPI, defined ................................................... 814
NSGP
about ................................................................. 344
defined .............................................................. 814
enabling access on device interface ...................... 226
overbilling .......................................................... 345
NSM reporting, configuring on device .................. 314
NSM, enabling access on device interface ............. 226
ns-profile ........................................................... 548
NSRP
defined .............................................................. 814
NSRP Monitor ..................................................... 708
RTOs, defined ..................................................... 817
statistics monitoring ............................................ 708
synchronizing cluster configurations ................... 382
NSRP clusters
about ................................................................. 376
active/active ........................................................ 381
configuring cluster .............................................. 376
creating cluster ................................................... 377
creating cluster with existing policy .................... 116
DIP groups ........................................................ 273
forcing cluster device mode .................................. 376
master/backup .................................................... 383
monitoring .......................................................... 708
RTO mirror groups .............................................. 383
RTOs ................................................................. 383
secure communications ...................................... 377
statistics ............................................................ 690
synchronizing ...................................................... 382
transparent mode ............................................... 377
VSD groups ........................................................ 381
VSiS ................................................................. 381
NSRP Monitor, permission to view ....................... 63
NTP
configuring on device ......................................... 308
server, configuring on device .............................. 308
synchronizing device clock .................................. 428
numbered tunnel interfaces ................................. 259
O
Object Manager
about ................................................................. 20
defined ............................................................. 814
objects
about ................................................................. 442
address ............................................................ 444
attacks, updating predefined ............................... 451, 455
attacks, viewing predefined .................................. 450
authentication servers ......................................... 498
AV profiles ........................................................ 478
certificate authorities .......................................... 517
CRLs ................................................................. 520
custom attack group ............................................ 474
custom attacks ..................................................... 456
custom attacks, compound ................................... 460
custom attacks, extended information .................... 458
custom attacks, external references ....................... 458
custom attacks, name and description .................... 457
custom attacks, protocol anomaly ......................... 459
custom attacks, signature ...................................... 459
custom attacks, target platform ............................. 459
custom compound attacks .................................... 471
custom compound attacks, adding members ........... 473
custom compound attacks, attack pattern ............... 473
custom compound attacks, ordered match .............. 473
custom compound attacks, scope ......................... 472
custom protocol anomalies ................................... 470
custom signature attack attack context .................. 465
custom signature attacks ...................................... 460
custom signature attacks, attack direction .............. 466
custom signature attacks, attack flow .................... 466
custom signature attacks, attack header matches ...... 467
custom signature attacks, attack pattern ............... 464
custom signature attacks, attack pattern syntax ...... 464
custom signature attacks, false positive setting ...... 460
custom signature attacks, first packet context ......... 466
custom signature attacks, IP header matches .......... 467
custom signature attacks, IP protocol and type ...... 461
custom signature attacks, line context ................... 466
custom signature attacks, packet context ............... 465
custom signature attacks, service binding .............. 460
custom signature attacks, stream 256 context ......... 466
custom signature attacks, stream context ............... 466
custom signature attacks, supported services .......... 462
custom signature attacks, TCP header matches ....... 468
custom signature attacks, time binding ................. 463
custom signature attacks, UDP header matches ...... 469
DIP profiles ........................................................ 451
DIP, global ........................................................ 451
group expressions ............................................... 516
group expressions, configuring ..................................... 513
GTP ........................................................................... 486
IKE proposals .............................................................. 523
imported ....................................................................... 443
IP pools ......................................................................... 511
MIP, global ..................................................................... 517
NAT .............................................................................. 516
permissions ..................................................................... 63
predefined attacks ....................................................... 449
protected resources ...................................................... 520
remote settings ............................................................. 515
schedules ........................................................................ 448
service groups ............................................................... 495
service objects in firewall rules ..................................... 540
services .......................................................................... 492
services, adding .............................................................. 494
services, custom ............................................................ 494
URL custom categories ................................................ 482
URL predefined categories ........................................... 483
users ............................................................................. 507
users, external ............................................................... 508
users, local ...................................................................... 507
VIP, global ....................................................................... 517
one-time-password ........................................................ 151
operation mode on WAP ............................................... 156
optimizing rulebases using reports ................................. 797
OSPF
about ............................................................................ 186
configuring areas ............................................................ 188
configuring authentication .............................................. 191
configuring interface link type ....................................... 190
configuring neighbors .................................................... 191
configuring parameters on virtual router ......................... 187
configuring redistribution rules ....................................... 189
configuring summary import ......................................... 188
configuring tunnel interface as demand circuit ................. 191
configuring virtual links ................................................ 189
defined ............................................................................ 814
enabling on device ........................................................ 186
ignoring MTU mismatch in DB exchange ......................... 190
not so stubby area (NSSA) ............................................ 188
reduce LSA flooding ....................................................... 190
stub area ......................................................................... 188
virtual link ....................................................................... 821
OTP.................................................................................. 151
overbilling ...................................................................... 345
overlapping subnets, ignoring on virtual router ................. 172

P
packet context ................................................................... 465
packet flow, configuring on device ................................. 466
password length, restricting .......................................... 303
passwords, device administrators .................................. 300
PAT
See port address translation
pattern file, updating on device ........................................ 426
peer ................................................................................. 814
perfect forward secrecy .................................................. 524
permit action, configuring in firewall rules ....................... 541
permitted IPs .................................................................... 301
PIM-SM
about ............................................................................ 203
acceptable groups ........................................................ 206
proxy rendezvous point ............................................... 207
rendezvous point to group mapping ................................. 205
ping, enabling access on device interface ......................... 226
PKI defaults
configuring on device .................................................... 373
revocation settings ......................................................... 374
SCEP ............................................................................. 375
polices
See security policies
policy name, ScreenOS ................................................. 553
policy validation tool ..................................................... 577
port mapping
See also NAT-dst
port mapping, defined ................................................... 815
port modes, defined ....................................................... 815
PPP................................................................................. 261
PPPoE
configuring on device .................................................... 286
See also ADSL
using on ADSL interface ................................................. 261
PPPoE, assigning to a VSI interface ................................. 279
automatic update of DNS servers ................................... 280
configuring on device .................................................... 279
defined ............................................................................ 815
multiple sessions on single interface ................................. 282
PPPoE, using on ADSL interface ....................................... 261
preamble settings on WAP ............................................... 159
predefined entities in templates ....................................... 135
predefined service timeouts, configuring on device ............ 331
preference, defined ......................................................... 815
preferred ID, configuring in firewall rules ......................... 547
prefixes, defined ............................................................ 815
prerequisite activities ..................................................... 60
preview tools ................................................................. 399
primary interface, fail over .............................................. 429
priority levels for traffic shaping ..................................... 335, 544
protected resources ....................................................... 520, 605
protocol anomaly attack objects, custom ......................... 470
protocol distribution
device-specific view, described ..................................... 689
viewing ......................................................................... 693–694
Protocol Independent Multicast-Sparse-Mode
See PIM-SM
public key authentication (PKA), device administrators ... 300
R
RADIUS
access-challenge, defined ............................................. 803
authentication server example ....................................... 503
authentication servers ................................................... 501–505
compatibility with RFC 2138 ......................................... 501
ranges ............................................................................ 747
reactivating settings on WAP ........................................... 166
Realtime Monitor module ................................................ 21
Index
rebooting devices ................................................................. 427
redistribution
defined ................................................................. 816
redistribution list .......................................................... 815
redundant interface .......................................................... 253
refreshing DNS entries on devices ........................................ 427
re-importing devices ........................................................ 35, 76, 395, 586
re-importing policies .......................................................... 586
reject action
changed to deny ............................................................. 579
configuring in firewall rules ................................................. 341
rekey ........................................................................... 623
remote authentication dial in user service
See RADIUS
remote settings ............................................................... 515
report groupings .............................................................. 782
Report Manager module .................................................. 18
report time period, configuring ............................................ 791
reporting options on device
email notification ............................................................ 313
messages and destinations ................................................. 313
SNMP ........................................................................... 314, 732
syslog ............................................................................ 314
Webtrends ........................................................................... 315, 734
reports
administrative ............................................................... 785
Attacks by Severity (DI) .................................................... 784
Attacks by Severity (Screen) ............................................... 785
Attacks over Time (DI) ....................................................... 784
Attacks over Time (Screen) .................................................. 785
configuring ................................................................. 790
DI ............................................................................... 784–785
FW/VPN ........................................................................ 784
historical ......................................................................... 800
Logs by User-set Flag ....................................................... 786
Screen ............................................................................... 786
Top Alarms ................................................................. 784
Top Attackers (Screen) ...................................................... 785
Top Attacks (DI) .............................................................. 784
Top Attacks (Screen) ........................................................ 785
Top Configuration Logs ................................................... 784
Top Information Logs ...................................................... 784
Top Rules ......................................................................... 786
Top Self Logs ................................................................. 784
Top Targets (Screen) ......................................................... 785
Top Traffic Alarms ........................................................... 784
Top Traffic Log ................................................................. 784
using to identify attack trends ........................................... 799
using to optimize rulebases ............................................. 797
using to track configuration changes ................................ 798
using to track incidents .................................................... 795
reset hardware (device) ...................................................... 303
resource statistics
device-specific view, described ......................................... 690
viewing ......................................................................... 702
restarting devices ............................................................ 427
reivation checking ............................................................ 519
RFC 2138, RADIUS compatibility ....................................... 501
RIP
about ............................................................................. 193
alternate routes per prefix .................................................. 194
configure tunnel interface as demand circuit ......................... 197
configuring authentication ................................................. 197
configuring neighbors ....................................................... 197
configuring parameters ..................................................... 194
configuring redistribution rules ........................................... 196
configuring summary import ............................................. 196
defined ........................................................................... 816
enable summarization ....................................................... 197
enabling ......................................................................... 193
hold down time .............................................................. 195
poll interval for demand circuits ........................................ 195
retransmit interval for demand circuits ................................ 195
split horizon ................................................................. 197
timers .............................................................................. 195
version on interface ......................................................... 197
version on virtual router instance ....................................... 194
role-based administration
about ............................................................................. 52
configuring ................................................................. 57
creating administrators ...................................................... 57
creating roles .................................................................... 60
creating subdomains ........................................................ 64
domain versioning ............................................................ 65
dependant activities .......................................................... 60
example ........................................................................... 66
using effectively ............................................................. 53
using, enterprise organizations ........................................... 54
using, service providers ................................................... 56
root administrator, setting on device .................................... 428
root device administrator .................................................... 298
route exporting ............................................................... 172
route flap dampening ....................................................... 816
route lookup preference ................................................... 171
route maps
about ............................................................................. 173
defined ........................................................................... 816
offset metric ..................................................................... 175
preserve preference ......................................................... 174
setting match conditions .................................................. 173
setting permitted route attributes ..................................... 174
route preferences, configuring on virtual router ..................... 185
route reflector ............................................................... 816
routes, about ................................................................. 170
routing
default route, defined ....................................................... 807
next hop ......................................................................... 813
prefecture ................................................................. 815
table, defined ............................................................... 816
Routing Information Protocol
See RIP
routing table entries
configuring ................................................................. 179
keep route active when interface is down ......................... 180
service binding
   selecting for custom attack object .................................. 460
   supported services .......................................................... 462
service objects
   about ........................................................................... 492
   configuring in firewall rules ........................................... 540
   custom ........................................................................ 494
   MS-RPC ....................................................................... 493
   Sun-RPC ...................................................................... 493
service options
   Ident-Reset .................................................................... 226
   NSGP .......................................................................... 226
   NSM ........................................................................... 226
   ping ............................................................................. 226
   SNMP ........................................................................... 226
   SSH ............................................................................ 226
   SSL ............................................................................. 226
   SSL HP ......................................................................... 307
   SSL Handshake Protocol
      See SSL HP
   SSL HP ......................................................................... 307
   SSL Handshake Protocol
      See SSL HP
   SSID ............................................................................... 160
   SSIDs on WAP ................................................................ 160
   service binding
      configuring ................................................................. 705
   session display filter
      configuring ................................................................. 705
   session filter
      active sessions, viewing ............................................... 704
   session rematch ................................................................ 581
   session timeout, idle timeout .......................................... 499
   SHA-1, defined ................................................................ 818
   short slots on WAP .......................................................... 159
   SIBR ............................................................................. 183
signature attack objects
   BugTraq references ........................................................ 459
   creating ICMP header properties .................................... 469
   custom ........................................................................... 460
   CVE references .............................................................. 458
   packet context ............................................................... 465
   viewing flow properties .................................................. 466
   viewing service binding ................................................... 462
Simple Certificate Enrollment Protocol
   See SCEP
SIP
   attack protection .......................................................... 332
   defined ......................................................................... 818
   destination IP server protection ...................................... 332
   incoming DIP for ............................................................ 244
   INVITE messages ........................................................... 332
   site survey ...................................................................... 167
   SMTP mail server, specifying on device .......................... 313
   sniffer Security Policy .................................................... 535
SNMP
   configuring on device .................................................... 314, 732
   creating communities ..................................................... 733
   enabling access on device interface ................................ 226
   private traps, configuring on virtual router ....................... 172
source interface-based routing table
   See SIBR
source NAT, configuring in firewall rules ............................ 542
source routing table ........................................................... 181
split DNS queries, configuring on device ......................... 289
SSH
   configuring on device .................................................... 304
   defined ......................................................................... 817
   enabling access on device interface ................................ 226
   port, configuring for device CLI management .................. 302
   SSHv1, configuring on device ......................................... 305
   SSHv2, configuring on device ......................................... 306
   SSLDs on WAP ................................................................ 160
   SSL
      configuring on device .................................................. 307
      disabling on device .................................................... 308
      enabling access on device interface ............................. 226
      redirection ................................................................. 307
      SSL HP ......................................................................... 307
      SSL Handshake Protocol
         See SSL HP
   SSL HP ......................................................................... 307
   SSL Handshake Protocol
      See SSL HP
   SSID ............................................................................... 160
   SSIDs on WAP ................................................................ 160
   sys time ........................................................................ 817
   syslog
      configuring on device .................................................. 314
      configuring syslog host ................................................. 314
      syslog, defined ........................................................... 819
      system clock, updating ............................................... 428
      system device-specific views ....................................... 690
      system statistics, viewing ............................................ 702
      system status monitor, permission to view .................... 64
T
   target platform for custom attack object ......................... 459
   TCP header matches for custom attack object ................. 468
   TCP MSS option ............................................................. 341
   TCP MSS, all option ....................................................... 341
   TCP MSS, GRE in .......................................................... 342
   TCP MSS, GRE out ........................................................ 342
TCP RST bit and sequence number, check ...........................................340
TCP RST invalid session.................................................................339
TCP sequence number check, skip..............................................338
TCP SYN bit before create session for tunneled packets, check .................339
TCP SYN bit before create session, check ........................................339
TCP/IP, defined ...........................................................................820
Telnet
  banner .................................................................................311
  enabling access on device interface ................................................226
  port, configuring for device CLI management ..................................302
templates.........................................................................................77
  about .........................................................................................133
  applying .....................................................................................151
  applying multiple templates .........................................................143
  benefits .....................................................................................133
  default values ............................................................................135
  derived values ...........................................................................134
device groups .................................................................................135
example applying ...........................................................................137
example creating ............................................................................136
example multiple templates .........................................................143
key list parameters ........................................................................136
limitations .......................................................................................135
maximum .......................................................................................135
modifying applied template .......................................................143
overriding .......................................................................................134
permissions ....................................................................................62
predefined entities ........................................................................135
security policy ..............................................................................535
setting priority ...............................................................................143
unsupported device options .........................................................140, 142
temporal key integrity protocol ....................................................165
TFTTP/FTP server, configuring on device .........................................343
time binding for custom attack object ............................................463
time, setting on device ....................................................................308
timeout for authentication user ......................................................499
TKIP ...............................................................................................165
toolbar in UI ..................................................................................17
Top Alarms report ..........................................................................784
Top Attackers (DI) report .......................................................784, 799
Top Attackers (Screen) report ......................................................785, 799
Top Attacks (DI) report .................................................................784
Top Attacks (Screen) report .......................................................785, 799
top axis, Log Investigator ..............................................................757
top Configuration Logs report ....................................................784, 798
top Information Logs report .......................................................784, 798
top Log report .................................................................................786, 797
Top Logs report .............................................................................786, 797
Top Self Logs report .......................................................................784
Top Targets (Screen) report .......................................................785, 799
Top Traffic Alarms report ...............................................................784
Top Traffic Log report ...................................................................784
tracking configuration changes, using reports ..................................798
tracking incidents, using reports ....................................................795
traffic device-specific views .........................................................689
traffic distribution
  by protocol, viewing .....................................................................693
  by security policy, viewing ...........................................................690
  by VPN, viewing ..........................................................................690
  for device, viewing .......................................................................690
traffic log report............................................................................784
traffic shaping
  about .........................................................................................543
  configuring on device .................................................................334
  DSCP class selector .....................................................................335, 544
  mode .........................................................................................335, 543
  transmission power level settings on WAP ..................................156
troubleshooting, sending commands to device ..................................706
trust zone, defined .........................................................................820
trustee privileges ...........................................................................298
tunnel interfaces
  about .........................................................................................258
  configuring for VPN ....................................................................608
  configuring single for ScreenOS 5.x .............................................615
defined ..........................................................................................820
  MTU size .....................................................................................260
tunnel zones
  configuring ..................................................................................608
defined ..........................................................................................820
U
UDP header matches for custom attack object ..................................469
unnumbered tunnel interfaces ......................................................259
untrust zone, defined ......................................................................820
updating attack object database ..................................................415
updating IDP engine .....................................................................46, 420
URL categories
  permission to update on device ..................................................62
  permission to update on system ..................................................64
  updating on device .....................................................................426
  updating on system ....................................................................426
URL filtering
  black list ......................................................................................484, 548
  block action ................................................................................484
  configuring in firewall rules ..........................................................548
  create custom category .................................................................482
  create custom profile ...................................................................484
  custom profiles ............................................................................484
  custom URL categories .................................................................548
  ns-profile .....................................................................................485
  permissions to update URL categories .........................................62
  permit action ...............................................................................484
  predefined profiles .......................................................................484
  predefined URL categories ..........................................................484, 548
  SurfControl CPA (Integrated) in rules ..........................................548
  SurfControl SCFP/WebSense (Redirect) in rules ..............................548
  white list ......................................................................................484, 548
user authentication, configuring in firewall rules ..................................550
user flag
  See flag
user group objects, configuring in firewall rules ..................................550
user objects
  about .........................................................................................507
  configuring in firewall rules ..........................................................550
  external .......................................................................................508
  local ..............................................................................................507
  using external user groups in VPNs .................................................508
  using MIPs as source or destination in firewall rules .......................538
V
vendor-specific attributes
  See VSAs .................. version of attack object database ............................................ 419
VIP options, configuring on device ........................................... 295
VIPS
  configuring in device .................................................. 233
  defined ................................................................... 821
  global objects ................................................................ 517
  mapping services and ports ............................................. 234
virtual IPs
  See VIPS ......................................................................
virtual link, defined ....................................................... 821
virtual routers
  about ........................................................................... 169
  access lists ................................................................. 172
  border gateway control
    See BGP
    configuring for vsys ................................................... 352
    configuring on device .............................................. 170
    configuring RIP .. ..................................................... 193
    consider active routes ............................................. 172
    destination-based routes .......................................... 180
    dynamic routing protocols ........................................ 185
    export and import rules .......................................... 175
    gateway tracking ...................................................... 181
    general properties ................................................... 171
    ignore overlapping subnets ....................................... 172
    maximum equal cost routes ....................................... 171
    maximum number of routes ....................................... 171
    multicast routing ..................................................... 201
    next-hop ................................................................. 172
    open shortest path first
      See OSPF
      route exporting ..................................................... 172
      route lookup preference ........................................... 171
      route maps ................................................................ 173
      route preferences .................................................. 185
      routing information protocol
        See RIP
        routing table entries ............................................. 179
        shared VR ................................................................ 171
        SNMP private traps .............................................. 172
        source interface-based routes .................................. 183
        source-based routes ............................................... 181
        synchronizing/unsynchronizing ................................ 382
        virtual router ID .................................................... 171
virtual security device groups
  See VSD groups
virtual security devices
  See VSD
virtual security interface
  See VSI
virtual link
  adding policy-based members ........................................... 19, 592
  adding RAS users ...................................................... 615
adding routing-based members .............................................. 615
adding the VPN ............................................................ 611
adding the VPN link ....................................................... 626
autogenerating VPN rules .................................................. 624
configuring ASN1-DN ..................................................... 621
configuring FQDN ......................................................... 622
configuring gateway ...................................................... 618
configuring gateway security ............................................ 620
configuring gateway, heartbeats ........................................ 618
configuring gateway, mode ............................................. 618
configuring gateway, NAT Traversal .................................... 619
configuring IKE IDs ...................................................... 621
configuring IKE properties ............................................. 622
configuring L2TP .......................................................... 614
configuring NAT ............................................................ 613
configuring NAT with incoming DIP ..................................... 613
configuring NAT with MIP, VIP, and Outgoing DIP ............... 613
configuring NAT with tunnel interface and zone .................. 613
configuring overrides .................................................... 624
configuring overrides, device configuration ......................... 625
configuring overrides, policy rules .................................... 624
configuring Phase 1 proposals .......................................... 620
configuring Phase 2 proposals .......................................... 623
configuring PKI ............................................................ 620
configuring preshared key ............................................... 620
configuring preshared secrets .......................................... 621
configuring translation points ........................................... 618
configuring topology ....................................................... 616
configuring topology, full mesh ......................................... 617
configuring topology, hub and spoke .................................. 617
configuring topology, main and branch ................................ 617
configuring topology, site-to-site ...................................... 617
configuring XAuth ........................................................ 619
creating VPNs ................................................................ 611
default termination point .................................................. 612
device tunnel summary ..................................................... 626
editing VPNs ................................................................. 626
enable dial backup .......................................................... 612
enabling a VPN ............................................................ 612
enabling VPN Monitor ..................................................... 623
enabling VPN Monitor, rekey ............................................ 623
examples ........................................................................ 628–650
expanded view .................................................................. 592, 627
view properties ............................................................... 612
VPN Monitor
  about .......................................................................... 706
  enabling ....................................................................... 623
  permission to view ...................................................... 64
VPN rules in firewall rulebase ............................................. 531
VPN status summary, viewing ............................................ 707
VPNs
  creating with VPN Manager ........................................... 611
  device-level, about ..................................................... 593
  device-level, adding VPN rules ....................................... 664
  device-level, AutoKey IKE VPNs .................................... 651
  device-level, L2TP VPNs ............................................. 662
  device-level, L2TP-over-AutoKey IKE VPNs ..................... 663
  device-level, manual key VPNs ....................................... 658
  device-level, supported configurations ................................ 650
display filter ................................................................. 708
<table>
<thead>
<tr>
<th>Index</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>distribution device-specific view</td>
<td>689</td>
</tr>
<tr>
<td>monitoring status</td>
<td>706</td>
</tr>
<tr>
<td>permissions</td>
<td>64</td>
</tr>
<tr>
<td>planning for</td>
<td>593</td>
</tr>
<tr>
<td>planning for, full mesh</td>
<td>596</td>
</tr>
<tr>
<td>planning for, hub and spoke</td>
<td>595</td>
</tr>
<tr>
<td>planning for, IPsec</td>
<td>597</td>
</tr>
<tr>
<td>planning for, L2TP</td>
<td>599</td>
</tr>
<tr>
<td>planning for, policy-based</td>
<td>600</td>
</tr>
<tr>
<td>planning for, route-based</td>
<td>601</td>
</tr>
<tr>
<td>planning for, site-to-site</td>
<td>594</td>
</tr>
<tr>
<td>preparing certificates</td>
<td>609</td>
</tr>
<tr>
<td>preparing group IKE IDs</td>
<td>607</td>
</tr>
<tr>
<td>preparing NAT objects</td>
<td>605</td>
</tr>
<tr>
<td>preparing protected resources</td>
<td>605</td>
</tr>
<tr>
<td>preparing RAS users</td>
<td>606</td>
</tr>
<tr>
<td>preparing VPN Components</td>
<td>604</td>
</tr>
<tr>
<td>supported configurations</td>
<td>593</td>
</tr>
<tr>
<td>tunneling, defined</td>
<td>820</td>
</tr>
<tr>
<td>VSAs</td>
<td></td>
</tr>
<tr>
<td>attribute name</td>
<td>503</td>
</tr>
<tr>
<td>attribute number</td>
<td>503</td>
</tr>
<tr>
<td>attribute type</td>
<td>503</td>
</tr>
<tr>
<td>NetScreen dictionary file</td>
<td>502</td>
</tr>
<tr>
<td>vendor ID</td>
<td>503</td>
</tr>
<tr>
<td>VSD groups</td>
<td>381</td>
</tr>
<tr>
<td>VSIs</td>
<td>252, 381</td>
</tr>
<tr>
<td>vsys</td>
<td></td>
</tr>
<tr>
<td>about</td>
<td>351</td>
</tr>
<tr>
<td>administrators</td>
<td>351</td>
</tr>
<tr>
<td>configuring interfaces</td>
<td>353</td>
</tr>
<tr>
<td>configuring virtual routers</td>
<td>352</td>
</tr>
<tr>
<td>configuring zones</td>
<td>353</td>
</tr>
<tr>
<td>read-only admins</td>
<td>299</td>
</tr>
<tr>
<td>viewing configuration</td>
<td>352</td>
</tr>
<tr>
<td>W</td>
<td></td>
</tr>
<tr>
<td>Web management, configuring on device</td>
<td>306</td>
</tr>
<tr>
<td>WebAuth</td>
<td></td>
</tr>
<tr>
<td>banners</td>
<td>311</td>
</tr>
<tr>
<td>configuring in firewall rules</td>
<td>550</td>
</tr>
<tr>
<td>Websense default port</td>
<td>324</td>
</tr>
<tr>
<td>WebTrends</td>
<td></td>
</tr>
<tr>
<td>configuring on device</td>
<td>734</td>
</tr>
<tr>
<td>defined</td>
<td>822</td>
</tr>
<tr>
<td>reporting, configuring on device</td>
<td>315</td>
</tr>
<tr>
<td>WebUI, enabling access on device interface</td>
<td>226</td>
</tr>
<tr>
<td>WEP keys on WAP</td>
<td>163</td>
</tr>
<tr>
<td>WEP settings on WAP</td>
<td>162</td>
</tr>
<tr>
<td>WIN5S, defined</td>
<td>822</td>
</tr>
<tr>
<td>wireless settings</td>
<td></td>
</tr>
<tr>
<td>about</td>
<td>153</td>
</tr>
<tr>
<td>aging</td>
<td>157</td>
</tr>
<tr>
<td>antenna</td>
<td>154</td>
</tr>
<tr>
<td>beacon</td>
<td>157</td>
</tr>
<tr>
<td>burst</td>
<td>157</td>
</tr>
<tr>
<td>channel</td>
<td>155</td>
</tr>
<tr>
<td>control frame protection</td>
<td>158</td>
</tr>
<tr>
<td>data rate</td>
<td>156</td>
</tr>
<tr>
<td>fragmentation</td>
<td>158</td>
</tr>
<tr>
<td>MAC access lists</td>
<td>159</td>
</tr>
<tr>
<td>operation mode</td>
<td>156</td>
</tr>
<tr>
<td>preamble</td>
<td>159</td>
</tr>
<tr>
<td>reactivating</td>
<td>166</td>
</tr>
<tr>
<td>short slots</td>
<td>159</td>
</tr>
<tr>
<td>SSIDs</td>
<td>160</td>
</tr>
<tr>
<td>transmission power level</td>
<td>156</td>
</tr>
<tr>
<td>WEP</td>
<td>162</td>
</tr>
<tr>
<td>WEP keys</td>
<td>163</td>
</tr>
<tr>
<td>WPA</td>
<td>165</td>
</tr>
<tr>
<td>WPA rekey</td>
<td>165</td>
</tr>
<tr>
<td>WPA-PSK passphrase</td>
<td>166</td>
</tr>
<tr>
<td>WPA-PSK pre-shared key</td>
<td>166</td>
</tr>
<tr>
<td>WLAN settings</td>
<td>153</td>
</tr>
<tr>
<td>WPA rekey settings on WAP</td>
<td>165</td>
</tr>
<tr>
<td>WPA settings on WAP</td>
<td>165</td>
</tr>
<tr>
<td>WPA-PSK</td>
<td></td>
</tr>
<tr>
<td>passphrase settings on WAP</td>
<td>166</td>
</tr>
<tr>
<td>pre-shared key on WAP</td>
<td>166</td>
</tr>
<tr>
<td>settings on WAP</td>
<td>165</td>
</tr>
<tr>
<td>X</td>
<td></td>
</tr>
<tr>
<td>X509 certificates</td>
<td>373</td>
</tr>
<tr>
<td>XAuth, defined</td>
<td>822</td>
</tr>
<tr>
<td>Z</td>
<td></td>
</tr>
<tr>
<td>zone</td>
<td></td>
</tr>
<tr>
<td>adding on device</td>
<td>212</td>
</tr>
<tr>
<td>configuring for vsys</td>
<td>353</td>
</tr>
<tr>
<td>configuring on device</td>
<td>212</td>
</tr>
<tr>
<td>device-specific views</td>
<td>690</td>
</tr>
<tr>
<td>exceptions in firewall rules</td>
<td>583</td>
</tr>
<tr>
<td>filters in rules</td>
<td>584</td>
</tr>
<tr>
<td>mismatch</td>
<td>577</td>
</tr>
<tr>
<td>statistics</td>
<td>702</td>
</tr>
<tr>
<td>tunnel</td>
<td>820</td>
</tr>
</tbody>
</table>