Contents

Preface ......................................................................................................................................................... 17
  Organization ............................................................................................................................................. 18
  NetScreen Publications ............................................................................................................................ 20

Section 1: Preparing .................................................................................................................................. 21

Introduction ............................................................................................................................................... 23

About NetScreen-Security Manager 2004 ................................................................................................. 24
  Security Integration ................................................................................................................................... 24
  Complete Support .................................................................................................................................... 24
  Network Organization ............................................................................................................................... 24
  Role-Based Administration ......................................................................................................................... 25
  Centralized Device Configuration .............................................................................................................. 25
  Migration Tools ........................................................................................................................................ 26
  Device Management ................................................................................................................................. 26
  Device Modeling ...................................................................................................................................... 26
  Rapid Deployment (RD) .............................................................................................................................. 27
  Policy-Based Management ........................................................................................................................ 27
  Error Prevention, Recovery & Auditing ....................................................................................................... 27
  Device Configuration Validation ............................................................................................................... 28
  Policy Validation ...................................................................................................................................... 28
  Atomic Configuration ............................................................................................................................... 28
  Device Image Updates ............................................................................................................................... 28
  Auditing .................................................................................................................................................. 28
  Complete System Management ................................................................................................................. 29
  VPN Abstraction ..................................................................................................................................... 29
  Integrated Logging & Reporting .................................................................................................................. 29
  Monitoring Status ................................................................................................................................. 30
  Job Management ...................................................................................................................................... 30

Technical Overview ................................................................................................................................... 31
  Architecture ........................................................................................................................................... 31
  UI ......................................................................................................................................................... 31
  Management System ............................................................................................................................. 32
  Managed Devices .................................................................................................................................... 34
  Distributed Data Collection ...................................................................................................................... 34
  Security .................................................................................................................................................. 35
  Scaling & Performance ............................................................................................................................ 35

Working in the User Interface .................................................................................................................... 36
  UI Overview .......................................................................................................................................... 36
  Navigation Tree ...................................................................................................................................... 37
  Main Display Area ................................................................................................................................. 37
  Menu Bar ............................................................................................................................................. 37
  ToolBar ............................................................................................................................................... 37
  Status Bar ............................................................................................................................................ 37
Security Manager Modules ................................................................. 37
Log Viewer ....................................................................................... 37
Report Manager ............................................................................. 38
Log Investigator .............................................................................. 38
Device Manager ............................................................................. 38
Policy Manager .............................................................................. 38
VPN Manager .................................................................................. 39
Object Manager .............................................................................. 39
Server Manager .............................................................................. 40
Realtime Monitor ............................................................................ 40
Job Manager ..................................................................................... 41
Audit Log Viewer ............................................................................ 41
Synchronizing UI Edits .................................................................... 41

Configuring Role-Based Administration (RBA) ........................................... 43

About Role-Based Administration (RBA) .................................................... 44
About Domains ................................................................................ 44
About Roles ..................................................................................... 45

Using Role-Based Administration Effectively ........................................... 46
Enterprise Organizations .................................................................. 46
Geographical Divisions .................................................................. 46
NOC & SOC .................................................................................... 47
Administrator Types ....................................................................... 47
Service Providers ........................................................................... 48
Internal Network ............................................................................ 48
Managed Security Service Provider (MSSP) .......................................... 48

Configuring Role-Based Administration .................................................. 50
Creating Administrators .................................................................... 50
Configuring General Settings .............................................................. 50
Configuring Authorization ................................................................ 51
Configuring Permissions ................................................................... 51
Creating Roles ................................................................................ 52
Creating Custom Roles ..................................................................... 52
Selecting Dependant Activities ........................................................... 54
Assigning & Viewing Custom Roles ..................................................... 54
Creating Subdomains ...................................................................... 55
Viewing Current Domain Detail .......................................................... 55
Domain Versioning .......................................................................... 55
Example RBA: Service Provider .......................................................... 56
Step 1: Create the Subdomains ............................................................ 56
Step 2: Create the Subdomain Administrator ......................................... 57
Step 3: Create the Viewing & Reporting Administrator ......................... 57
Step 4: Verify Administrator Accounts ............................................... 59

Planning Your Security Manager Network ............................................. 62
Creating a Network ......................................................................... 62
Modeling New Devices ..................................................................... 62
Importing Existing Devices ............................................................... 63
Simplifying Management ................................................................. 64
Using Device Groups ....................................................................... 65
Using Device Templates ................................................................... 65
Merging Policies .............................................................................. 65
Section 2: Integrating

Adding Devices

About Device Creation .............................................................. 70
  Determine Device Status ...................................................... 70
  Verify Device Configuration ................................................. 71
  Managing the Device .......................................................... 71

Before You Begin ..................................................................... 72
  ScreenOS Version? ............................................................... 72
  Import or Model? ................................................................. 72
  Importing Device Configurations ......................................... 72
  Modeling Device Configurations ......................................... 72
  Global Domain or Subdomain? ............................................... 73
  Using Devices in VPNs .......................................................... 73
  Selecting the Domain .......................................................... 73

Importing Devices .................................................................. 75
  Overview ............................................................................. 75
  Requirements ...................................................................... 75
  Adding Devices with Static IP Addresses ................................. 75
    ScreenOS 4.0.x Devices ...................................................... 76
    ScreenOS 5.0.0 Devices ...................................................... 77
  Adding Devices with Dynamic IP Addresses ............................ 78
    ScreenOS 4.0.x Devices ...................................................... 78
    ScreenOS 5.0.0 Devices ...................................................... 80
  Verifying the Imported Device Configuration .......................... 81
    Using Job Manager .......................................................... 81
    Using Device Monitor ....................................................... 81
    Using the Device Manager ............................................... 81
    Using Configuration Summaries ....................................... 82

Modeling Devices .................................................................... 84
  Overview ............................................................................. 84
  Requirements ...................................................................... 84
  Modeling a Device .............................................................. 84
  Creating Device Configuration ............................................ 85
  Activating Devices ............................................................ 85
  Devices with Static IP Addresses ......................................... 85
  Devices with Dynamic IP Addresses ................................. 87

Configuring Devices for Rapid Deployment .............................. 90
  Overview ............................................................................. 90
  Requirements ...................................................................... 91
  Creating the Configlet .......................................................... 91
  Installing the Configlet ......................................................... 93
  Preparing the Device .......................................................... 93
  Installing the Configlet ......................................................... 93
  Updating the Device Configuration ....................................... 95
Contents

Adding Other Device Types ................................................................. 96
  Adding Vsx Devices ........................................................................ 96
  Placing the Root Device ................................................................. 96
  Importing Vsx Devices .................................................................... 97
  Modeling Vsx Devices ..................................................................... 98
  Adding an Extranet Device ............................................................. 99
  Adding a Cluster ............................................................................ 99
  Adding a Cluster Device Object ....................................................... 99
  Adding Members to the Cluster ....................................................... 100

Configuring Devices ........................................................................ 101

About Device Configuration .............................................................. 102
  Changes that Affect NSM-Device Connection .................................. 102
  Configuring Devices in Device Manager ......................................... 102
  Templates ..................................................................................... 103
    Creating Templates ....................................................................... 103
    Example: Creating and Applying a Template ................................. 105
    Validating Template Information .................................................. 107
    Modifying Fields in a Template ..................................................... 107
    Applying Multiple Templates to a Device ...................................... 108
    Example: Creating and Applying Multiple Templates .................... 108
  Device Groups ............................................................................... 116

Configuring Device Information ......................................................... 117
  Configuring Startup Information ................................................... 117
  Applying Templates ....................................................................... 117
  Viewing Device Capabilities .......................................................... 118

Configuring Network Settings .......................................................... 119
  Configuring the Network Module ................................................... 120
  Configuring Virtual Routers ........................................................... 120
    Adding Custom Virtual Routers .................................................... 120
    Configuring Virtual Router Parameters ....................................... 120
    Configuring Virtual Router General Properties ............................ 121
    Configuring Access Lists ............................................................ 122
    Configuring Route Maps ............................................................. 122
    Configuring Export and Import Rules .......................................... 123
    Configuring Routing Table Entries .............................................. 124
    Configuring Route Preferences .................................................... 126
    Configuring Dynamic Routing Protocols ...................................... 126
  Configuring Zones ....................................................................... 130
    Adding a Security or Tunnel Zone ................................................ 130
    Configuring Zone Parameters ..................................................... 131
  Configuring Interfaces .................................................................. 131
    Adding Interfaces ....................................................................... 131
    Configuring Interface Parameters .............................................. 132
  Configuring DIP Groups ................................................................ 133
  Configuring PPPoE ...................................................................... 133
  Configuring NACN ...................................................................... 134
  Configuring Interface Failover ...................................................... 135
  Configuring a Modem Connection ................................................ 135
    Creating Modem Settings ............................................................ 136
    Creating ISP Settings .................................................................. 136
Configuring DNS ................................................................. 137
Configuring Advanced Network Settings ................................. 137
  Configuring ARP Cache Entries ........................................... 137
  VIP Options .................................................................... 138
  Configuring DIP Options ................................................. 138

Configuring Device Administration ........................................... 139
  Configuring Date and Time Settings ..................................... 139
  Configuring Management .................................................. 139
  Configuring Banners ....................................................... 140
  Configuring Default Servers ............................................. 140

Configuring Reporting ................................................................ 141
  Configuring General Reporting Options ............................... 141
  Configuring Email Notification ......................................... 141
  Configuring NSM Reporting .............................................. 142
  Configuring SNMP Reporting ............................................ 142
    Creating SNMP Communities ......................................... 142
  Configuring Syslog Reporting ............................................ 143
  Configuring a Syslog Host ............................................... 143
  Configuring Webtrends Reporting ....................................... 143

Configuring Security ................................................................ 145
  Configuring Antivirus (AV) Settings .................................... 145
  Configuring External AV Scanners ...................................... 145
  Configuring the Internal AV Scanner ................................... 146
  Configuring Webmail Scanning ......................................... 146
  Configuring URL Filtering ............................................... 147
  Configuring Deep Inspection ............................................ 147
  Configuring the Attack Database ........................................ 148

Configuring Advanced Device Settings ..................................... 149
  Configuring Timeouts for Predefined Services ....................... 149
  Configuring SIP Settings ............................................... 149
  Configuring Traffic Shaping ............................................. 150
  Configuring Packet Flow ................................................ 151
  Configuring TFTP/FTP Server Operation ............................. 151
  Configuring Host and Domain Name .................................... 151

Configuring L2TP/XAuth/Local Users ....................................... 153

Configuring vsys ................................................................. 154
  Configuring Virtual Routers for a vsys .............................. 154
  Configuring Zones for a vsys .......................................... 154
  Configuring Interfaces for a vsys ...................................... 155
  Viewing vsys on the Root Device ...................................... 155

Configuring Certificates ...................................................... 156
  Configuring a Local Certificate ........................................ 156
    Generating the Certificate Request ................................. 157
    Obtaining and Installing the Certificate .......................... 157
  Configuring CA Certificates ............................................ 159
    Using SCEP ................................................................ 159
    Manually .................................................................... 159
  Configuring CRLs ............................................................ 160

NetScreen-Security Manager 2004 7
Using Imported Certificates .................................................. 160
Configuring PKI Defaults .................................................... 160
Configuring X509 Certificates ............................................... 161
Configuring Revocation ...................................................... 161
Configuring SCEP ............................................................. 162
Configuring NSRP Clusters ................................................... 163
Creating an NSRP Cluster .................................................... 163
Adding Member Devices to the Cluster ................................. 164
Configuring Active/Active Operation .................................... 164
Synchronizing Configurations .............................................. 165
Forcing Master/Backup State .............................................. 165

Updating Devices .................................................................. 167

About Updating ................................................................. 168
About Updating Tools ......................................................... 168
About the Update Process .................................................... 169

Knowing When to Update .................................................. 172
Checking Device Status ...................................................... 172
Checking Error Log Entries ............................................... 173
Checking for Administrative Changes ................................. 174
Reviewing Reports ............................................................ 174

Using Preview Tools .......................................................... 175
Using a Configuration Summary ........................................... 175
Running a Configuration Summary ..................................... 176
Using a Delta Configuration Summary ............................... 177
Running a Delta Configuration Summary ......................... 178

Updating Devices ............................................................. 179
Updating Multiple Devices .................................................. 179
Updating Device Groups ..................................................... 180
About Atomic Configuration .............................................. 180

Tracking Device Updates with Job Manager ......................... 181
Using the Job Manager ...................................................... 181
About the Job Information Window ................................. 182
Understanding Update Device States ................................. 184
Understanding Errors in the Update Process ...................... 185

Section 3: Managing .......................................................... 187

Managing Devices ........................................................... 189

Upgrading Firmware on Devices ......................................... 190
Loading Image Files ......................................................... 190
Upgrading the Firmware on Devices ................................. 190
Adjusting the Firmware Version ........................................ 191

Installing and Displaying License Keys ............................... 192
Installing License Keys ..................................................... 192
Displaying License Key Information .................................. 192
Activating Subscription Services ........................................... 193
  Retrieving a Service Subscription........................................ 193
Updating the Attack Database .................................................. 194
  Updating the Database Immediately ........................................ 194
  Checking the Attack Database Version .................................... 194
Updating AV Pattern Files ...................................................... 195
  Updating the AV Pattern File ............................................... 195
Miscellaneous Device Operations ............................................ 196
  Restarting Devices ......................................................... 196
  Refreshing DNS Entries ................................................... 196
  Updating the Device Clock with an NTP Server ......................... 196
  Setting the Root Administrator on a Device ............................ 197
  Failing Over/Reverting Back Interfaces .................................. 198
  Setting RMA State on a Device ........................................... 198
  Troubleshooting a BGP Peer Session on a Device ...................... 199
  Displaying CLI Commands on a Device ................................... 199
  Finding Usages ............................................................. 199
Managing Device Capabilities ................................................. 200
  Abstract Data Model ....................................................... 200
  Data Model ............................................................... 201
  Data Model Schema ....................................................... 201
  Data Model Updating ...................................................... 201
  Device Model Importing ................................................... 203
Configuring Objects ............................................................ 205
  About Objects .............................................................. 206
    Object Types ............................................................ 206
    Imported Objects ....................................................... 207
  Configuring Address Objects .............................................. 208
    Viewing Address Objects ............................................... 208
    Creating Address Objects .............................................. 208
      Adding a Host Address Object ....................................... 209
      Adding a Network Address Object ................................... 209
      Adding an Address Object Group .................................... 209
  Configuring Schedule Objects ........................................... 211
    Creating Schedule Objects ............................................ 211
  Configuring Attack Objects .............................................. 212
    Attack Object Types ................................................... 212
      Signature Attack Objects .......................................... 212
      Protocol Anomaly Attack Objects .................................. 212
      Predefined & Custom Attack Objects ................................ 213
    Viewing Predefined Attack Objects .................................. 213
    Updating Predefined Attack Objects .................................. 213
    Creating Custom Attack Objects ...................................... 214
    Creating Attack Groups ............................................... 215
  Configuring AntiVirus Objects ............................................ 216
Configuring Firewall Rules .......................................................... 245
  Defining Match ........................................................................ 245
  Source & Destination Zones ...................................................... 245
  Source & Destination Address Objects ...................................... 245
  Services .................................................................................. 246
  Defining Actions ...................................................................... 247
  Selecting Devices ..................................................................... 248
  Configuring Rule Options .......................................................... 248
    Enabling NAT ......................................................................... 248
    Configuring Traffic Shaping ................................................... 249
    Enabling Logging & Counting ................................................ 250
    Miscellaneous ....................................................................... 251
    Authentication ...................................................................... 252
    AntiVirus ............................................................................. 253
    Configuring Attack Protection ............................................... 253
    Comments ........................................................................... 254

Validating Firewall Policies ......................................................... 255
  Using the Policy Validation Tool ................................................ 255
    Rule Shadowing .................................................................... 255
    Unsupported Options ............................................................. 256

Installing & Updating Firewall Policies ......................................... 257
  Before Installing Policies .......................................................... 257
  During Policy Installation .......................................................... 257
  Updating Policies ..................................................................... 258

Managing Rules & Policies .......................................................... 259
  Using Zone Exceptions ............................................................. 259
  Using Zone Filters .................................................................... 259
  Editing Rule Order .................................................................... 259
  Using Cut, Copy, & Paste .......................................................... 259
  Deleting a Rule ........................................................................ 259
  Disabling a Rule ....................................................................... 260
  Merging Policies ....................................................................... 260
    Example: Policy Merge .......................................................... 261

Configuring VPNs ....................................................................... 263

About VPNs .............................................................................. 264
  Creating System-Level VPNs with VPN Manager ...................... 264
  Creating Device-Level VPNs in Device Manager ....................... 265
  Supported VPN Configurations ................................................. 265

Planning for Your VPN ............................................................... 266
  Determining Your VPN Members & Topology ............................ 266
    Using Network Address Translation (NAT) ............................. 266
    Site-to-Site ........................................................................... 266
    Hub & Spoke ........................................................................ 267
    Full Mesh ............................................................................ 268
  Creating Redundancy ................................................................. 268
  Protecting Data in the VPN ....................................................... 269
    IPSec .................................................................................. 269
    L2TP .................................................................................. 271
Choosing a VPN Tunnel Type .................................................. 271
Policy-Based ................................................................. 272
Route-Based ................................................................. 272
VPN Checklist ............................................................... 273
Members & Topology ........................................................ 273
Policy-Based, Route-Based, or Mixed-Mode ............................ 273
Security Protocol (Encryption & Authentication) .................... 274
VPN Manager or Device-Level? ........................................... 274

Preparing VPN Components ............................................... 276
Basic VPN Components ..................................................... 276
Required Policy-Based VPN Components ............................. 276
Configuring Address Objects .............................................. 277
Configuring Protected Resources ....................................... 277
Configuring Shared NAT Objects ....................................... 278
Configuring Remote Access Service (RAS) Users ................... 278
Required Routing-Based VPN Components ......................... 279
Configuring Tunnel Interfaces & Tunnel Zones ....................... 280
Configuring Static & Dynamic Routes ................................. 280
Optional VPN Components .............................................. 281
Creating Authentication Servers ....................................... 281
Creating Certificate Objects ............................................. 281
Creating PKI Defaults ..................................................... 281

Creating VPNs with VPN Manager ....................................... 283
Adding the VPN ............................................................. 283
Configuring Members ..................................................... 284
Adding Policy-Based Members .......................................... 284
Adding RAS Users ......................................................... 286
Adding Routing-Based Members ....................................... 286
Configuring Topology ..................................................... 287
Defining Topology ......................................................... 287
Defining Termination Points ............................................ 288
Configuring Gateways .................................................... 289
Configuring Gateway Properties ....................................... 289
Configuring Gateway Security .......................................... 291
Configuring IKE IDs ....................................................... 292
Configuring IKE ........................................................... 292
IKE Properties ............................................................. 293
Configuring Security Level .............................................. 294
Autogenerating the VPN ................................................... 294
Configuring Overrides ..................................................... 295
Editing Policy Rules ....................................................... 295
Editing Device Configuration ......................................... 296
Viewing the Device Tunnel Summary ................................. 296
Adding the VPN Link ....................................................... 297
Editing VPNs ............................................................... 297
Editing VPN Protected Resources ..................................... 297
Editing the VPN Configuration ....................................... 297
Editing VPN Overrides ................................................... 297

VPN Manager Examples ................................................... 298
AutoKey IKE, Policy-Based Site-to-Site VPN ......................... 298
Step 1: Create VPN Components ..................................... 298
Step 2: Create the VPN ................................................... 301
Step 3: Configure the VPN ......................................................... 301
Step 4: Add the VPN Link ...................................................... 304
AutoKey IKE RAS, Policy-Based VPN ....................................... 304
Step 1: Create VPN Components ............................................. 305
Step 2: Create the VPN ........................................................... 308
Step 3: Configure the VPN ...................................................... 309
Step 4: Add the VPN Link ...................................................... 311
AutoKey IKE, Route-Based Site-to-Site VPN ............................. 312
Step 1: Create VPN Components ............................................. 312
Step 2: Create the VPN ........................................................... 314
Step 3: Configure the VPN ...................................................... 314
Step 4: Create Routes ............................................................ 318

Creating Device-Level VPNs .................................................. 323
Supported Configurations ..................................................... 323
Creating AutoKey IKE VPNs .................................................... 323
Configuring Gateways .......................................................... 323
Configuring Routes (Route-based only) ..................................... 327
Configuring the VPN ........................................................... 328
Adding a VPN Rule ............................................................. 330
Creating Manual Key VPNs .................................................... 331
Adding XAuth Users ............................................................ 331
Configuring Routes (Route-based only) ..................................... 331
Configuring the VPN ........................................................... 331
Adding a VPN Rule ............................................................. 333
Creating L2TP VPNs ............................................................ 334
Adding L2TP Users ............................................................. 334
Configuring L2TP ............................................................... 334
Adding a VPN Rule ............................................................. 335
Creating L2TP Over Autokey IKE VPNs .................................... 335
Adding VPN Rules ............................................................. 335
Configuring the VPN ........................................................... 336
Configuring the Firewall Policy .............................................. 336
Assign & Install the Firewall Policy ........................................ 336

Section 4: Monitoring ........................................................... 337

Monitoring ........................................................................... 339

About Realtime Monitor ......................................................... 340
Realtime Monitor Views ......................................................... 340
Monitoring FW/VPN Devices .................................................. 341
Viewing Device Status .......................................................... 341
Device Polling Intervals ......................................................... 342
Viewing Additional Device Detail and Statistics .......................... 344
Viewing Device Details .......................................................... 344
Viewing Device Statistics ...................................................... 345

Monitoring VPNs ................................................................... 369
Viewing the VPN Status Summary ........................................... 369
Configuring a VPN Display Filter ............................................ 370
Viewing Active VPN Details ................................................... 370
Viewing Device-Specific VPN Information ............................... 370

NetScreen-Security Manager 2004
## Monitoring NSRP Statistics
- Viewing NSRP Summary Information .............................................................. 371
- Viewing VSD/RTO Information ......................................................................... 372
- Viewing VSD Counter Details ........................................................................... 373
- Viewing RTO Counter Details .......................................................................... 373

## Using The Realtime Monitor
- Example: Monitoring Device Status ................................................................. 374

## Logging ........................................................................................................... 375

### About Logging ............................................................................................. 376
- About Logs ........................................................................................................ 376
- Log Categories ................................................................................................. 377
- Log Severity Levels ......................................................................................... 377
- About Log Modules ......................................................................................... 378
- About Log Volumes .......................................................................................... 378
- Understanding Log Flow .................................................................................. 379

### Managing Log Volume .................................................................................. 380
- Archiving Logs .................................................................................................. 381
- Purging Logs .................................................................................................... 381
- Exporting Logs ................................................................................................ 381

### Configuring Logging ...................................................................................... 382
- About Log Types .............................................................................................. 382
- Configuring Device-Level Logging .................................................................... 383
  - Configuring SCREEN Logs ............................................................................ 384
  - Configuring Self Logs .................................................................................. 385
  - Forwarding Logs to Other Destinations ....................................................... 386
- Configuring Logging in Firewall Rules .............................................................. 389
  - Configuring Traffic Logs ............................................................................ 389
  - Configuring Alarm Logs .............................................................................. 391
  - Configuring Anomaly Logs ......................................................................... 391
  - Configuring Signature Logs ........................................................................ 392
  - Configuring Custom Attack Logs ................................................................. 393
- Configuring the GUI Server for Logging .......................................................... 394
  - Configuring Log Actions ............................................................................. 394
  - Log Criteria .................................................................................................. 395
- Other Log Types ............................................................................................... 395
  - Information Logs .......................................................................................... 395
  - Configuration Logs ...................................................................................... 396

### Using the Log Viewer .................................................................................... 397
- About the Log Viewer ....................................................................................... 397
- Log Viewer Columns ....................................................................................... 398
- Log Viewer Summary ....................................................................................... 400
- Managing Logs ................................................................................................. 401
  - Using Flags .................................................................................................. 402
  - Using the Find Utility ................................................................................. 403
  - Locating Logs By ID Number ....................................................................... 403
  - Using Filters ................................................................................................ 403
- Searching with Ranges .................................................................................... 410
Using Log Views ............................................................................................................. 413
Saving Views ..................................................................................................................... 413
Exporting Views ............................................................................................................... 413
Customizing Columns ....................................................................................................... 414
Example: Customizing Columns ....................................................................................... 414
Fine-Tuning with the Log Viewer ...................................................................................... 416
Jump to Policy ..................................................................................................................... 416
Identify Irrelevant Attacks ................................................................................................. 416
Jump to Device Configuration ............................................................................................ 417

Using the Log Investigator ............................................................................................... 418
Working with Log Investigator Data .................................................................................. 420
Configuring the Log Investigator ...................................................................................... 422
Setting the Number of Data Points on Each Axis ............................................................. 422
Selecting Data ...................................................................................................................... 422
Selecting By Individual Cells ............................................................................................ 423
Selecting Axes ...................................................................................................................... 423
Benefits/Limitations of Different Analysis Levels ............................................................. 424
Setting Log Investigator Parameters ............................................................................... 425
Configuring a Time Interval .............................................................................................. 425
Configuring a Beginning Time ........................................................................................... 425
Setting the Data Type ........................................................................................................ 426
Setting a Log Entry Limit ................................................................................................... 426
Zooming on Data ................................................................................................................. 427
Jumping to the Log Viewer ............................................................................................... 427
About Zoom In Data ............................................................................................................ 427
Log Investigator Example ................................................................................................. 428
Excluding Log Investigator Data ....................................................................................... 429
Setting Filters for Log Investigator Data .......................................................................... 430

Using the Audit Log Viewer ............................................................................................. 432
Configuration Administration Settings .............................................................................. 433

Reporting .......................................................................................................................... 435

About Reporting ................................................................................................................ 436
Report Type Groupings ...................................................................................................... 436
Graphical Data Representation ......................................................................................... 437
Integration with Logs ......................................................................................................... 438
Central Access to Management Information ...................................................................... 438
Report Types ...................................................................................................................... 439
FW/VPN Reports ................................................................................................................ 439
DI Reports ........................................................................................................................... 439
Screen Reports .................................................................................................................... 440
Administrative Reports ..................................................................................................... 440
Setting Report Options ...................................................................................................... 441
Configuring a Report Time Period .................................................................................... 441
Configuring the Data Point Count .................................................................................... 441
Configuring the Chart Type .............................................................................................. 441
Log Viewer Integration ...................................................................................................... 442
Contents

Using Reports ................................................................. 443
  Example: Using Administrative Reports to Track Incidents .............. 443
  Example: Using Administrative Reports to Optimize Rulebases ......... 444
  Example: Using FW/VPN Report to Track Configuration Changes ...... 445
  Example: Using Screen Reports to Identify Attack Trends .............. 446
  Example: Using Deep Inspection Reports to Detect Application Attacks ... 446
Using Historical Reports ..................................................... 448

Glossary i

Unmanaged Commands xiii
NetScreen-Security Manager 2004 is a software application that helps you centralize control and management of your NetScreen security devices. With Security Manager, NetScreen delivers integrated, policy-based security and network management for all NetScreen products.

Security Manager uses the technology developed for ScreenOS 5.0 to simplify management support, enabling support for previous and future versions of ScreenOS. By integrating management of all NetScreen FW/VPN devices, Security Manager enhances the overall security of the Internet gateway.

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

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.
ORGANIZATION

This manual has 1 preface, 4 sections, 12 chapters, a glossary, an appendix, and an index.

Section 1: Preparing

Chapter 1, “Introduction” details 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 Security Manager UI.

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

Section 2: Integrating

Chapter 3, “Adding Devices” details how to add NetScreen FW/VPN devices to Security Manager. This chapter also describes how to use Rapid Deployment (RD) to quickly deploy devices in non-technical environments.

Chapter 4, “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.

Section 3: Management

Chapter 5, “Updating Devices” details how to use configuration summaries, update your device configurations, and use Job Manager to track the update progress.

Chapter 6, “Managing Devices” details how to maintain device features, manage device images, and update AntiVirus and Deep Inspection files on the device.

Chapter 7, “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 8, “Configuring Firewall Policies” details how to build firewall rules and create efficient firewall policies.

Chapter 9, “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.

Section 4: Monitoring

Chapter 10, “Monitoring” details the firewall, VPN, and NSRP monitoring functionality of Security Manager.

Chapter 11, “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 12, “Reporting” details how to create reports from log information.
**Glossary**
The glossary defines terms and concepts used in the Security Manager environment.

**Appendix**
The appendix details unsupported ScreenOS CLI commands.

**Index**
The index provides an alphabetical list of the major topics and subtopics discussed in this document, and their corresponding page numbers.
NETSCREEN PUBLICATIONS

To obtain technical documentation for any NetScreen product, visit www.netscreen.com/support/manuals.html. To access the latest NetScreen documentation, see the Current Manuals section. To access archived documentation from previous releases, see the Archived Manuals section.

To obtain the latest technical information on a NetScreen product release, see the release notes document for that release. To obtain release notes, visit www.netscreen.com/support and select Software Download. Select the product and version, then click Go. (To perform this download, you must be a registered user.)

If you find any errors or omissions in the following content, please contact us at the e-mail address below:

  techpubs@netscreen.com


SECTION 1: PREPARING
Introduction

In This Chapter:

- About NetScreen-Security Manager 2004
- Technical Overview
- Working in the User Interface

All networks are different, but each network is built the same way: You devote time to
design your network, spend money to buy the necessary equipment, and put in the hard
work to build and customize your network components so they work the way you want
them to. In an ideal world, that would be the end of the job—the perfect network has
perfect uptime, with perfect redundancy, growth potential, etc.

The reality is that managing your network devices is a full-time job. Ensuring that all
devices in your system are up and running, patched against vulnerabilities and exploits,
and functioning as expected requires a team of intelligent and committed individuals who
understand every aspect of their network. To respond quickly and appropriately to a
network situation, IT administrators, network administrators, and security
administrators must have complete control over network connectivity, network access,
and network traffic flow.

As your network grows, individual device maintenance can quickly become a logistical
nightmare. New devices, new networking technologies, software upgrades—almost every
change to your network requires some human and monetary resource. Even in small
networks, setting up and maintaining each device individually is time-consuming, prone
to error, and likely to require network downtime. Many organizations are now turning
towards integrated management solutions to help them configure and manage devices
more efficiently.

Security Manager is designed to give you back complete control over your network. The
concept is simple: Using Security Manager, you can configure all your NetScreen FW/VPN
devices from one location, at one time. Security Manager manages the functionality of
ScreenOS and incorporates Global Pro functionality in one unified system with a single,
streamlined User Interface.
ABOUT NETSCREEN-SECURITY MANAGER 2004

At its foundation, a management system integrates your individual FW/VPN devices into a single, effective security system that you control from a central location. With 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.

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 NetScreen FW/VPN devices. The management system tracks and logs each administrative change in realtime, providing you with a complete administrative record and helping you perform fault management.

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 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 Security Manager, this location is the Security Manager UI, a graphical user interface that contains a virtual representation of every NetScreen FW/VPN 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 NetScreen FW/VPN devices or systems. 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 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 Security Manager—define strategic roles for your administrators, delegate management tasks, and enhance existing permission structures with new task-based functionality.

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

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

- **Administrators.** An administrator is a user of 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, like read/write administrator, read-only administrator, or security 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. (31 maximum).

- **Shared Objects.** An object is a 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.
Chapter 1 Introduction

The global domain is a good location for FW/VPN 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, address objects, etc. 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 policy creation and deployment, and enable group-specific reporting. You can even link groups using Group Expressions to create a custom, dynamic group.

**Migration Tools**

If you have existing NetScreen FW/VPN devices deployed on your network or are using a previous NetScreen management system, you can use the Security Manager migration tools to quickly import your existing FW/VPN devices and their configurations, address books, service objects, policies, VPNs, and administrator privileges. As 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 NetScreen FW/VPN device, or from your Global Pro or Global Pro Express system. Import all your FW/VPN 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, Security Manager automatically transfers your existing domain structure.

For details on migrating from a previous management system, see the NetScreen-Security Manager Migration and Installer's 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. 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. 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 Security Manager, you can implement a new routing protocol across your network, design and deploy a new firewall 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 NetScreen FW/VPN devices in a large networked environment with minimal user involvement. RD is designed to simplify the staging and configuration of FW/VPN devices in non-technical environments, enabling the secure and efficient deployment of a large number of devices.

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

RD is ideal for quickly bringing new NetScreen FW/VPN devices under 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 Security Manager.

**Policy-Based Management**

Create simplified and efficient firewall policies for your managed devices using:

- **Groups.** Group your devices by platform, ScreenOS version, location, or function, then add them to your firewall policies.
- **Zone Exceptions.** To simplify your firewall rule, 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 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 FW/VPN rule.

**Error Prevention, Recovery & 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 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 Security Manager. Additionally, you can track each change made by an Security Manager administrator to help you identify when, how, and what changes were made to your managed devices.
Device Configuration Validation

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.

Policy Validation

The policy validation tool checks your firewall policies and alerts you to possible problems before you install that policy on your managed devices.

Atomic Configuration

On devices running ScreenOS 5.0, 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 Security Manager always maintains a stable connection to the managed device.

Device Image Updates

You can update the software that runs on your devices by installing a new ScreenOS image on all your NetScreen FW/VPN devices:

- **Security Manager updates.** Use Security Manager to upload the new image file to multiple NetScreen FW/VPN devices with a single click.
- **RMA updates.** To replace failed devices, set the modeled device to the RMA state, which enables 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.

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
- Security Manager admin 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 what changed from the previous version.
Complete System Management

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 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 a system, create templates and use them to quickly configure multiple, define 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 protocols such as 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 policies 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 & Reporting

You use the NetScreen FW/VPN 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 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 for 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

Security Manager can help you keep up-to-date on the health of your security system.

- View critical information about your device in the Device Monitor:
  - Configuration and connection status of your NetScreen FW/VPN 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 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. 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, 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
**Technical Overview**

Security from bottom up—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 Security Manager architecture and help with setting up the management system, see the NetScreen-Security Manager Installer's Guide.

**Architecture**

Security Manager is a three-tier management system comprised of a User Interface, management system, and managed devices (NetScreen FW/VPN 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 don't need LDAP or an external database.

![Security Manager Architecture Diagram]

**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 Windows (XP, NT, 2000) computers on your network. You use the UI to remotely access the management system.
Multiple Security Manager admins can interact with NetScreen FW/VPN devices using the UI, and can even configure unique UI preferences. The 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 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 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 NetScreen FW/VPN 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 Security Manager “management system”.

**GUI Server**

The GUI Server manages the system resources and data that drives Security Manager functionality. You can install the GUI Server software on a separate computer running Red Hat Linux 8/9 or Solaris 8/9, or on a Global Pro appliance. The GUI Server contains the Security Manager databases, and centralizes information for devices, their configurations, attack and server objects, and policies. Specifically, the GUI Server:

- Centralizes device, policy, and VPN configuration
- Organizes log entries from NetScreen FW/VPN devices for presentation
- Simplifies object management
• Manages multiple devices, networks, and domains
• Stores Security Manager administrator accounts and remote access user accounts

The GUI Server receives device information from the Device Server on a single inbound port and stores the data in its local database. When you use the UI to access 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>
<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 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 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 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 physically a separate GUI Server and multiple Device Servers 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 policy on that firewall to permit Security Manager management traffic.
When you start the Device Server, it runs the following processes:

<table>
<thead>
<tr>
<th>Process</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>devSvrManager</td>
<td>Device Server Manager enables FW/VPN devices to connect to and communicate with the Security Manager management system. The Device Server Manager is also responsible for writing log data into the local data store, and routing 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 FW/VPN 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 FW/VPN device that is enabled to work with Security Manager.</td>
</tr>
<tr>
<td>devSvrLogWalker</td>
<td>Device Server Log Walker performs user-specified actions on log entries (i.e., indexing, de-duplication, filtering).</td>
</tr>
</tbody>
</table>

**Managed Devices**

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

NetScreen Security Manager can manage NetScreen FW/VPN devices running ScreenOS 5.0.0 and ScreenOS 4.0.x (except 4.0.2). All devices from the NetScreen-5XT to the NetScreen-5400 are supported, except the NetScreen-5, NetScreen-10, and NetScreen-1000. Security Manager also supports the NetScreen-5GT running ScreenOS 4.0.0-DIAL2.

Security Manager also manage vsys configurations, NSRP clusters, and extranet devices.

**Distributed Data Collection**

The distributed data collection system provides Security Manager with a robust yet lightweight method for managing a variety of objects. In 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 updating 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. Security Manager uses capability files to enable NetScreen software upgrades without changing the device configuration in Security Manager.

**Security**

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, 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.

**Scaling & Performance**

Security Manager is designed to grow with your network, so you can continue to manage all your NetScreen network devices with Security Manager. As you add devices or network components to your physical network, you also add them to your virtual Security Manager network, where you can manage all future configurations. A 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 Security Manager User Interface (UI) is used to control the Security Manager system. Using the UI, you can configure Security Manager administrators, add devices, edit policies, view reports—access the full functionality of the Security Manager system.

**Note:** For step-by-step instructions on using the User Interface, click the icon in the menu bar of the UI to access the NetScreen-Security Manager Online Help.

**UI Overview**

The 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 Security Manager modules in the left pane of the 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 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.

Security Manager Modules
The Navigation Tree contains 11 top-level modules that contain specific Security Manager functionality, as detailed in the following sections.

Log Viewer
The Log Viewer displays log entries that your NetScreen FW/VPN devices generate based on criteria that you defined in your firewall 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
Chapter 1 Introduction

- 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 11, “Logging”.

Report Manager

The Report Manager contains summary, graphs, and charts that detail specific security events that occur on your network. 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 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 NetScreen FW/VPN devices. You can create:
- **NetScreen FW/VPN devices and systems.** The devices you use to enable access to your network and to protect your network against malicious traffic.
- **vsys devices.** A vsys is a virtual device that exists within a physical NetScreen FW/VPN device.
- **Clusters.** A cluster is two NetScreen FW/VPN devices joined together in a high availability configuration to ensure continued network uptime.
- **Extranet devices.** Firewalls or VPN devices that are not NetScreen devices.
- **Templates.** A template is a 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.

Policy Manager

Policy Manager contains the firewall 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 NetScreen FW/VPN devices.
Use Policy Manager to:

- Add or modify existing firewall policies
- Add or modify existing VPN rules
- Create new policies based on existing policies
- Install policies on one or multiple NetScreen FW/VPN devices
- Delete policies

If the device configurations that you imported from your NetScreen FW/VPN devices contained policies, Policy Manager displays those imported policies. For details on editing those imported policies or creating new policies, see Chapter 8, “Configuring Firewall Policies” or Chapter 9, “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 firewall 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 Security Manager system. An object is a re-usable, basic 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 Security Manager:

- **Address Objects** represent components of your network (hosts, networks, servers, etc.)
- **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.
- **Attack Objects** represent attack signatures and protocol anomalies used in Deep Inspection.
- **AV Objects** represent the servers that contain your virus definitions and AntiVirus software.
• **Service Objects** represent services running on your network, such as FTP, HTTP, and Telnet. 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 FW/VPN 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 Security Manager admins, 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.

• **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 7, “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 Security Manager system.

**Realtime Monitor**

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

• **Device Monitor** tracks the connection state and configuration state of your FW/VPN 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
- Update information at specified time periods
- Set alarm criteria for a device or process

For more details on Realtime Monitor, see Chapter 10, “Monitoring”.

**Job Manager**

Job Manager contains the status of commands (also called directives) that Security Manager sends to your managed devices. You can view summaries or details for active jobs and completed jobs.

**Audit Log Viewer**

The Audit Log Viewer contains a log for every change made by a Security Manager administrator.

**Synchronizing UI Edits**

When multiple Security Manager admins are accessing the Security Manager system at the same time, Security Manager synchronizes their edits 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 Security Manager admin begins editing an object, the UI locks that object to prevent other admins from editing the object’s value.
- During lockout, Security Manager makes “lazy” saves of all edits made and stores them in an in-memory database. If Security Manager crashes during a lazy save, edits made since the last lazy save are lost, and Security Manager prompts the 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.

For example, let’s say Bob and Carol are both Security Manager admins with the same roles. If both admins view the same object, but Bob also edits and saves the object, 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.
Configuring Role-Based Administration (RBA)

In This Chapter:

- About Role-Based Administration (RBA)
- Using Role-Based Administration Effectively
- Configuring Role-Based Administration
- Planning Your Security Manager Network

This chapter details how to use 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 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 Security Manager. Security Manager includes many features specifically designed for managing multiple NetScreen FW/VPN devices, such as device groups, templates, etc.
ABOUT ROLE-BASED ADMINISTRATION (RBA)

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 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 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 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.

Security Manager contains a default top-level domain, called the global domain, which can contain additional domains, called subdomains. Subdomains separate that exist within your larger network. 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 2004

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.
About Roles

Roles define who can perform which task and view which information. 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 Security Manager functionality.

All Security Manager users are some type of admin. During Security Manager installation, you are prompted for a password for the (default) admin account for 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 Security Manager functionality for the entire Security Manager system, a single domain, or specific functionality within a domain.

You can define multiple 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 Security Manager; the 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 Security Manager functionality for the entire Security Manager system, a single domain, or even specific functionality within a domain. You can even delegate Security Manager administrator management, enabling existing Security Manager administrators to create other 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). Because a device administrator does not use Security Manager to configure devices, you do not create an Security Manager administrator account for the device admin.
USING ROLE-BASED ADMINISTRATION EFFECTIVELY

The structure of your 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 recreate this same permission structure in 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.

**Enterprise Organizations**

Each enterprise defines administrative roles differently. With 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 & 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 firewall 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:

- The 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, etc.). Within the IT group, the network administrator might also have a role with an activity for managing the management system.
- The Security group creates and manages firewall policies. This group has roles with activities for defining custom services, address objects, and firewall policies on devices for which they have responsibility.
- The 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 FW/VPN 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 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” on page 48.

MSSPs can also use Virtual Systems (available on NS-FW 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.
Chapter 2 Configuring Role-Based Administration (RBA)

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 Security Manager administrators for those subdomains. When you create 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 & Domains to display the role-based administration settings for Security Manager:

- **Administrators.** Configure administrators for Security Manager.
- **Roles.** View or edit default roles, or create your own custom roles for your 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:** If you are migrating from Global Pro or Global Pro Express, you can migrate your existing domain structure and administrators. For details, see the NetScreen-Security Manager 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 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 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, etc.) for the new administrator.
Configuring Role-Based Administration

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

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

**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 Security Manager functionality, NetScreen recommends that you consider the security of the super administrator password appropriately. If you forget or lose the super administrator password, please contact NetScreen 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 Security Manager functionality. When you assign a role to an 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. 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 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” on page 52.

**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” on page 55.

Creating Roles

Click the Roles tab to display available roles. 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 exactly level of permission you want to give an admin. An activity is a predefined task that defines access to a function in Security Manager. To assign one or more activities to an Security Manager admin, create a role that includes those activities and assign the role to the admin.

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

<table>
<thead>
<tr>
<th>Function</th>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admins</td>
<td>View, Create, Edit, Delete</td>
<td>An admin is a user of the Security Manager management system.</td>
</tr>
<tr>
<td>Admin Roles</td>
<td>View, Create, Edit, Delete</td>
<td>An admin role defines the access privileges for a Security Manager administrator.</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>
| Devices, Device Groups, & Templates | View, Create, Edit, Delete | • A device is a NetScreen FW/VPN device.  
• A device group is a collection of managed devices.  
• A template is a device configuration that contains predefined, static configuration information, such as networking settings, interface settings, or DNS settings. |
<p>| Device Certificates       | Generate &amp; Upload, Get, Edit, Delete | A device certificate authenticates packets passing through a device. |</p>
<table>
<thead>
<tr>
<th>Function</th>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 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 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 Security Manager.</td>
</tr>
<tr>
<td>Device Firmware Update</td>
<td>Update</td>
<td>The device firmware is the ScreenOS software image used on the managed device.</td>
</tr>
<tr>
<td>Device Configuration</td>
<td>View Update</td>
<td>A device configuration is the modeled configuration that exists for a managed device within Security Manager.</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>Subdomains &amp; Groups</td>
<td>View Create</td>
<td>A subdomain is a separate, unique representation of other networks that exist within your larger network.</td>
</tr>
<tr>
<td></td>
<td>Edit Delete</td>
<td></td>
</tr>
<tr>
<td>System Error Logs View</td>
<td>View</td>
<td>A system error log displays information about a system error.</td>
</tr>
<tr>
<td>Historical Log Reports</td>
<td>View</td>
<td>An historical log report is a report generated using historical log entries.</td>
</tr>
<tr>
<td>Investigative Log Reports</td>
<td>View</td>
<td>An investigative log report is generated using the Log Investigator.</td>
</tr>
<tr>
<td>Active Jobs</td>
<td>Cancel</td>
<td>An active job is a task that Security Manager is currently performing, such as rebooting, updating, or firmware change. Active jobs display in the Job Manager.</td>
</tr>
<tr>
<td>Jobs</td>
<td>View</td>
<td>A job is a task that Security Manager can perform.</td>
</tr>
<tr>
<td>Device Logs</td>
<td>View Hide &amp;</td>
<td>A device log records a security event that occurred on a FW/VPN device.</td>
</tr>
<tr>
<td></td>
<td>Unhide Purge</td>
<td></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, etc. to a device log.</td>
</tr>
<tr>
<td>Device Status Monitor</td>
<td>View</td>
<td>The device status monitor tracks the status NetScreen FW/VPN devices, VPN tunnels, and NSRP.</td>
</tr>
<tr>
<td>Implicit</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Migration</td>
<td>N/A</td>
<td>Migration is the ability to migrate data from a Global Pro system to Security Manager 2004.</td>
</tr>
</tbody>
</table>
Some activities are dependant on other activities. If you select a dependant activity, 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.

### Assigning & 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.

## 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 authentication server for the global domain and for each subdomain. The default auth server is used:

- To authenticate administrators when they log into the Security Manager system
- To authenticate RAS users in VPNs

To create a default auth server, you must first use the Object Manager to create an Authentication Server object that represent the IP address, etc. for the server. After the server object is created, you can then select it as the default auth server.

## Domain Versioning

Each time you update a device configuration on a NetScreen FW/VPN device using Security Manager, a new version of the device domain is automatically created. 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; Security Manager displays the archived domain version as a read-only domain.
An archived domain version displays the modules (Device Manager, Policy Manager, Log Investigator, etc.) 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.

**Example RBA: Service Provider**

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, but 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)

The following sections detail each step.

**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. From the Menu bar, click Tools > Manage Domains & Administrators.

2. Click the Subdomains tab, then click the Add icon to create a subdomain for the first customer. Configure four subdomains total, as shown below:

3. 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). Security Manager loads the subdomain.
2. From the Menu bar, click Tools > Manage Domains & 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 to select a role and domain as shown below:

4. Click OK to save your changes.
5. Repeat for each subdomain.

Step 3: Create the Viewing & 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). Security Manager loads the subdomain.
2. From the Menu bar, click Tools > Manage Domains & 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 to select a role and domain as shown below:

6. Click OK to save your changes and return to the Administrators tab, which should display the following administrators:

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 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, password, and GUI Server IP address as shown below:

Click OK to login. The 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, customer admin name, password, and GUI Server IP address as shown below:
Click OK to login. The Security Manager Navigation Tree and main display area appear, as shown below:

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.
**Planning Your Security Manager Network**

After you have configured domains, roles, and administrators, the next step in using Security Manager to manage your NetScreen FW/VPN devices is to create a virtual network in Security Manager 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.

Some questions you might want to consider include:

- Where should you start and why?
- What is the best order to do things? Why?
- Are you building a new network? Are you importing an existing network?
- How do you use Security Manager to improve your existing network structure?
- How do you use management features to simplify your day-to-day administrative tasks?

The following sections provide information to help you decide how best to create your virtual network and simplify management tasks.

**Creating a Network**

You have two options for creating your virtual network:

- **Model** devices in Security Manager. If you do not have NetScreen FW/VPN devices deployed on your network, you can create device configurations in Security Manager. When you physically deploy your devices, you can install the modeled device configurations on those devices to instantly get them up and running.

- **Import** devices into Security Manager. If you have NetScreen FW/VPN devices deployed on your network, you should import and verify their device configurations.

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

**Modeling New Devices**

For new networks or networks that do not use a previously deployed NetScreen 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 Security Manager:

1. Create the domain structure that best suits your network topology and access requirements.
2. Create 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, designate virtual routers, etc. 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.
   - For ScreenOS 5.0 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 Firewall 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 (Security Manager includes an object database of common transport and application-level services).
   - AV objects for detecting viruses in your network traffic

5. Create Firewall Policies
   - Add a policy and create firewall rules that specify source, destination, service, action, etc. 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 Policies
   - 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 3, “Adding Devices”; for details on configuring devices, see Chapter 4, “Configuring Devices”.

**Importing Existing Devices**

For networks with deployed NetScreen FW/VPN 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.
Before you begin importing devices, however, you should review the import process thoroughly to understand how Security Manager will handle your configuration data, and to select the best method for importing your own individual security devices to Security Manager.

In general, the import process includes two concepts: importing information and verifying information. An overview of this process is provided below.

1. Import your device configuration directly from the device. As Security Manager imports your existing device configurations, it automatically creates your virtual network based on the configuration information.

2. Verify your imported device configuration:
   - Run a Delta Config Summary and view the results
   - Check Device configuration information
   - Check Address, Service, Schedule, and NAT Objects
   - Check Firewall Policies
   - Check Protected Resources
   - Check VPN Policies

3. Correct any validation errors, if found.

4. Check for duplicate objects (address objects, custom service objects, etc.). Be sure to consolidate any duplicate object before importing another NetScreen FW/VPN device.

You can also delete devices from 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 Security Manager system.

For details on importing devices, see Chapter 3, “Adding Devices”.

**Simplifying Management**

When you add your FW/VPN devices to Security Manager, you are creating the network organization that you will 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 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 Security Manager management features.

These features include:

- Using Device Groups
- Using Device Templates
- Merging Policies
Using Device Groups

You can create groups of devices to help you 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, virtual routers, etc., 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 NS-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 31 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 Security Manager UI and deploy them with a single click. Alternatively, Security Manager can import all existing policies from your FW/VPN device. You can import all security and access policies from your NetScreen FW/VPN devices, and import all VPN tunnels (route-based and policy-based) from your NetScreen FW/VPN devices.

Each time you import a policy from a managed device, that policy appears in Security Manager as a separate, individual policy in the Firewall Policies list. To simplify policy management and maintenance, you can merge two policies into a single policy. For details on merging policies, see Chapter 8, “Configuring Firewall Policies”.
SECTION 2: INTEGRATING
Adding Devices

In This Chapter:

- About Device Creation
- Before You Begin
- Importing Devices
- Modeling Devices
- Configuring Devices for Rapid Deployment
- Adding Other Device Types

Devices are the NetScreen security devices (FW/VPN devices) that you use to enable access to your network components and to protect your network against malicious traffic.

NetScreen Security Manager can manage NetScreen FW/VPN devices running ScreenOS 5.0.0 and ScreenOS 4.0.x (except 4.0.2). All devices from the NetScreen-5GT to the NetScreen-5400 are supported, except the NetScreen-5, NetScreen-10, and NetScreen-1000. Security Manager also supports the NetScreen-5GT running ScreenOS 4.0.0-DIAL2. Security Manager can also manage vsys configurations, NSRP clusters, and extranet devices.

Before you can manage a device with Security Manager, you must add the device to the management system.

Use Rapid Deployment (RD) to quickly add devices in non-technical environments with no staging requirements.
Chapter 3 Adding Devices

About Device Creation

Before Security Manager can manage your 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 the following types of devices:

- **NetScreen FW/VPN devices and systems** (NetScreen-5GT, NetScreen-208, etc.). The “Importing Devices” and “Modeling Devices” sections of this chapter detail how to add an existing or new NetScreen FW/VPN device into Security Manager.

- **vsys devices**. A vsys is a virtual device that exists within a physical NetScreen FW/VPN device. For details on adding vsys devices, see “Adding Vsys Devices” on page 96.

- **Clusters**. A cluster is two NetScreen FW/VPN devices joined together in a high availability configuration to ensure continued network uptime. For details on adding clusters, see “Adding a Cluster” on page 99.

- **Extranet devices**. Firewalls or VPN devices that are not NetScreen FW/VPN devices. For details on adding extranet devices, see “Adding an Extranet Device” on page 99.

To add any device type, you must determine the device status before you add the device, then verify the device configuration after the device is added to Security Manager.

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 5.0 or earlier version of ScreenOS, and have already been configured with an IP address, zones, etc. For deployed devices, you can import the existing device configuration information into 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, etc. 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, device admin name and password, etc., then uses that information to enable the physical device to connect to the Device Server.

After the physical device has connected, it is considered a managed device, meaning it is now under the control of the Security Manager.
Verify Device Configuration

For managed devices that use imported device configurations, you will want to 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 Security Manager device configuration (this summary is known as a Delta Configuration Summary). It's also a good idea to check your imported firewall policies, objects, and VPNs to become familiar with how the Security Manager UI displays them.

For managed devices that use modeled device configurations, you will want to verify that all device information was pushed to the physical device correctly. To identify discrepancies, you can 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 you have successfully added a device, you can begin managing its device configuration, objects, and 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 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 Security Manager system. However, during re-import, Security Manager imports all device configuration data—not just the data that was changed; any changes that exist in the modeled configuration will be lost during re-import. Additionally, after re-importing a device configuration, you must reassign the imported firewall policy to the device.

If you delete a device that was added using Rapid Deployment (described on page 90), you must also re-create the configlet and install it again on the device.
Before You Begin

Before you add a device to Security Manager, you should check the ScreenOS version that is running on the device, decide if you will import or model the device, and determine the location (global domain or subdomain) for the device.

ScreenOS Version?

Ensure that the devices you are adding to Security Manager are running a supported version of ScreenOS. Security Manager supports devices running 4.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 NetScreen customer support for details.

Import or Model?

Decide if you want to import or model your devices in Security Manager.

Importing Device Configurations

If you are currently using NetScreen FW/VPN devices in your existing network, you can add these devices into 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, etc.

After you have imported several devices, you can start using system-level management features, such as the policy merge tool (merge several device firewall 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).

Modeling Device Configurations

For new or undeployed NetScreen FW/VPN devices, you can add and configure the device into Security Manager and activate when you are ready to deploy the physical device on your network. Before connecting to the device, simply create a device (using the Add Device Wizard) that represents the ScreenOS platform and NetScreen FW/VPN device type of the actual, physical device. Next, model the device configuration in the Security Manager UI. Configure zones, interfaces, virtual routers, policies, logging features—all device 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, etc.) and objects (re-usable, custom objects such as NAT objects, CA certificates, etc.). For large deployments that involve multiple devices in non-technical environment, use Rapid Deployment (RD) to bring new FW/VPN devices under Security Manager management for initial configuration.
Global Domain or Subdomain?

Determine the domain you want the device to exist in. A domain is a logical grouping of devices, their policies, and their access privileges. 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.

Using Devices in VPNs

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. 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. An example is shown below:

Selecting the Domain

When you log in to the UI for the first time after installing the management system, 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 Security Manager before adding devices to that subdomain. For details on creating new subdomains, see “Configuring Role-Based Administration” on page 50. After you have created the subdomain, select it from the domain menu and begin the device creation process.

Note: 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.
**Importing Devices**

Security Manager can import device configurations from devices running ScreenOS 5.0 or earlier. The process differs slightly for 5.0 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 5.0 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; a single, always-on connection exists between the management system and the device.

**Overview**

Adding a deployed device to 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 Security Manager.

**Requirements**

To import a device:

- The physical device must have Telnet or SSH enabled.
- You must have the device connection information (IP address, etc.) and device admin name and password available.
- The device must be staged, meaning it is connected to your network and has network connectivity.
- The device must have at least one interface that has an IP address.
- Devices that use dynamically assigned IP address must also support NACN.
- Ensure that the device is operating in the desired mode. You cannot change the operational mode after importing the device into Security Manager.

**Adding Devices with Static IP Addresses**

A static IP address is an IP address that does not change.
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 NetScreen FW/VPN device.
   - Enter the username of the device admin.
   - Enter the password for the device admin.
   - Select the connection method (Telnet, SSH version 1, SSH version 2).
   - If you selected Telnet, click Next and goto 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 Security Manager Device Server IP address and port.
   - Use a MIP to configure the device to connect to the Security Manager Device Server through a mapped IP address and port.
   - Click Next.
5. Select Enable Logging to enable 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.

**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 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 5.0.0 Devices**

To import a ScreenOS 5.0.0 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 NetScreen FW/VPN device.
   - Enter the username of the device admin.
   - Enter the password for the device admin.
   - Select the connection method (Telnet, SSH version 1, SSH version 2).
   
   If you selected Telnet, click Next and goto 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.
5. Click Finish to complete the Add Device wizard. The new device appears in the Device Manager list.
6. 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.

7. 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.

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 Security Manager Device Server IP address and port. Use a MIP to configure the device to connect to the 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 Security Manager to collect log entries from the device.
   - Enter the username and password of the device admin.

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.
   - 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 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 5.0.0 Devices

To import a ScreenOS 5.0.0 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 Security Manager Device Server IP address and port. Use a MIP to configure the device to connect to the 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. 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.
   - 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 Security Manager management on the device.
5. Click Finish to complete the Add Device wizard. The new device appears in the Device Manager list.
6. 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.
7. 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.

**Verifying the Imported Device Configuration**

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

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

**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 the Device Manager**

In the FW/VPN Device tree, ensure that the device exists, then open the device configuration and check the following values:

- Ensure that the device serial number matches the physical device.
- Ensure that the device IP address matches the IP address for the physical device.
- Ensure that device administrator name and password are correct for the physical device.
- Ensure that the interface on the device are correct for the physical device.
- Browse the device configuration tree and ensure that the management system successfully imported all device configuration information, including zones, virtual routers, and routes.
Using Configuration Summaries

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.

**Note:** Configuration summaries are helpful tools for ongoing device maintenance, too, particularly for devices on which a local device administrator has performed 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 FW/VPN devices to which you have access. Select the device you just imported and click OK. Security Manager analyzes the UI device configuration and generates a summary report that lists the CLI commands that will be sent 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 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 FW/VPN devices to which you have access. Select the device you just imported and click OK. 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 deltas differences exist between the configuration on the physical device and the configuration in the UI. Security Manager automatically imports your VPNs and displays the VPN policies; however, 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 FW/VPN devices to which you have access. Select the device you just imported and click OK. 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 Security Manager then install that device configuration on the physical device. For ScreenOS 5.0 devices, you can use Rapid Deployment (RD) to quickly provision multiple devices in non-technical environments. See “Configuring Devices for Rapid Deployment” on page 90 for details.

**Note:** To quickly add multiple devices, use templates. For details, see Configuring Devices.

**Overview**

Adding an undeployed device to Security Manager is a four stage process:

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

**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.
- The device must be staged, meaning it is connected to your network and has network connectivity.
- 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.
4. Enable transparent mode, if desired. 

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

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

6. 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 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, interfaces, etc.) that is available for import. You can create a configuration for the device in Security Manager, then install that configuration on the device.

Double-click the device object to display the device configuration and begin configuring the device as desired. For details on device configuration, see Chapter 4, “Configuring Devices”.

### Activating Devices

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 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 NetScreen FW/VPN device.
   - Enter the device admin name and password.
Chapter 3 Adding Devices

Select the connection method (Telnet, SSH version 1, SSH version 2).
If you selected Telnet, click Next and goto 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 Security Manager Device Server IP address and port.
   - Use a MIP to configure the device to connect to the Security Manager Device Server through a mapped IP address and port.

5. Click Next. Select Enable Logging to enable 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.
   - 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.

   **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 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 5.0.0 Devices**

To activate a ScreenOS 5.0.0 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 NetScreen FW/VPN device.
   - Enter the device admin name and password.
   - Select the connection method (Telnet, SSH version 1, SSH version 2).
     - If you selected Telnet, click Next and goto 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 Security Manager to collect log entries from the device.
   - Enter the username and password of the device admin.

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.
   - 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 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 5.0.0 Devices**

To activate a ScreenOS 5.0.0 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 “Configuring Devices for Rapid Deployment” on page 90.)
4. Click Next.
   - Specify the First Connection One Time Password (OTP) that authenticates the device.
   - 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 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.
Chapter 3 Adding Devices

**CONFIGURING DEVICES FOR RAPID DEPLOYMENT**

Rapid Deployment (RD) enables deployment of multiple NetScreen appliances 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 Security Manager management for initial configuration

RD typically involves two people: The Security Manager administrator, who creates the necessary device configuration for the new firewall devices in the Security Manager management console, and the on-site admin, who enables the firewall device to contact Security Manager for configuration.

The **Security Manager administrator** works in the NSM 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 NetScreen firewall can contact your 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 NetScreen FW/VPN 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 NetScreen FW/VPN 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 Security Manager Device Server, enabling Security Manager to begin managing the device.

After the firewall device has connected to Security Manager, the Security Manager administrator can manage the device exactly like any other firewall in Security Manager.

**Note:** If you delete the NetScreen FW/VPN device from the Security Manager system then re-add the device, you must also re-create the configlet and install it on the physical device.

**Overview**

The Security Manager administrator adds a 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 (on page 95)

The sections below detail each stage.
Requirements

To use rapid deployment:

- The device must be running ScreenOS 5.0
- The device must use default factory settings.
- The device must be able to reach the Internet using a static IP address, a PPPoE-assigned IP address, or DHCP-assigned IP address.
- The device must be modeled in Security Manager system. For details on modeling a device, see "Modeling a Device" on page 84

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.
   - The wizard automatically selects the interface on the device that will connect to the 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 Security Manager Device Server IP address and port. Use a MIP to configure the device to connect to the Security Manager Device Server through a mapped IP address and port.
5. Click Next.
   - 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 device installation.
     - For devices with PPPoEs, you can pre-define the user name and password OR ask the on-site admin to specify the user name and password during device installation.
Chapter 3 Adding Devices

- For devices that use DHCP, the configlet automatically handles IP assignment during 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 installation.

- Specify the password for the configlet, or use the default device password (which is netscreen).
- Specify Device User Names and passwords, or use the default admin name and passwords for the device.
- 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 regenerate 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 RD Getting Started Guide available on the NetScreen-Security Manager Documentation CD. This guide provides step-by-step instructions for connecting a FW/VPN 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.
Configuring Devices for Rapid Deployment

Installing the Configlet

The on-site admin performs RD in two stages:

- Preparing the FW/VPN Device
- Installing the Configlet

The sections below detail each stage. For detailed, step-by-step instructions on installing the configlet, please see the RD Getting Started Guide.

Preparing the Device

Before you install the configlet, you must prepare the FW/VPN device:

1. Connect the device to your network. For details on connecting the device, see the User’s Guide that came with your FW/VPN 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 NetScreen FW/VPN devices running ScreenOS 5.0. 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 NetScreen FW/VPN 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 FW/VPN device.
2. In a Web browser, enter the IP address of the trust interface on the FW/VPN 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.
Chapter 3 Adding Devices

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 FW/VPN device for Security Manager management.

4. If prompted, enter the configlet password and click Next. The configlet password is given to you by the 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 Security Manager administrator included ISP information in the configlet, the RD Wizard displays that information. Ensure that all information is correct.

If the 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.

6. Click Next to initiate the connection to Security Manager.

The FW/VPN device connects to the Security Manager Device Server. During this first connection, the device and the Security Manager Device Server exchange authentication information. After 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 FW/VPN device erases the one-time-password (OTP) from memory.

7. Click close to exit the RD Wizard.

The Security Manager admin can now configure the device using Security Manager.

**Note:** If the configlet fails, you must reset the device to factory defaults. For details, see the User’s Guide that came with your NetScreen FW/VPN device.
Configuring Devices for Rapid Deployment

NetScreen-Security Manager 2004
**Adding Other Device Types**

You can also add or import other device types into Security Manager, such as vsys devices, clusters, and extranet devices.

**Adding Vsys Devices**

A Virtual System (vsys) is a virtual device that exists within a physical NetScreen FW/VPN device. The vsys device functions as a completely separate FW/VPN device. The physical device, called the root device, can contain multiple vsys devices. The following NetScreen systems can be root devices:

- NetScreen-500
- NetScreen-5000
- 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:
Importing Vsys Devices

Importing vsys devices is a two stage process:

- **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” on page 75.

- **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. 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 75 or “Modeling Devices” on page 84.

- **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 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 an Extranet Device**

An extranet device is a firewall or VPN device that is not a NetScreen FW/VPN device. If you use devices from multiple manufacturers, you can add extranet devices to Security Manager to represent your heterogeneous network environment. After you have added the extranet device to the Security Manager UI, you can use the device in groups, firewall 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 Security Manager UI.
- **IP Address.** Enter the IP Address of the extranet device

Click OK to add the extranet device to Security Manager.

**Adding a Cluster**

A cluster is a two NetScreen FW/VPN 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:

- Add the cluster device object.
- Add the members of the cluster to the cluster device object.

**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.
Chapter 3 Adding Devices

- **Physical Choice.** Select the NetScreen 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 a cluster member, the Add Device Wizard automatically imports the device configuration from the physical device.
- When modeling a cluster member, ensure that both cluster members have been added to the cluster device object before configuring the cluster.
In This Chapter:

- About Device Configuration
- Configuring Device Information
- Configuring Network Settings
- Configuring Device Administration
- Configuring Reporting
- Configuring Security
- Configuring Advanced Device Settings
- Configuring vsys
- Configuring Certificates
- Configuring NSRP Clusters

This chapter describes the Device Manager, the Security Manager module that enables you to configure NetScreen FW/VPN devices.

There are some device configurations that can only be performed by the device administrator via the CLI or WebUI. You 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

**Note:** Use the Policy Manager to configure firewall and VPN rules that control traffic on your network, as described in Chapter 8, “Configuring Firewall Policies”. Use the VPN Manager to configure VPNs, as described in Chapter 9, “Configuring VPNs”.

ABOUT DEVICE CONFIGURATION

The Device Manager module in Security Manager enables you to configure the managed FW/VPN devices in your network. You use the Device Manager to edit configurations after you add and import a device or to create configurations when you model a device. For details about adding or modeling a device, see Chapter 3, “Adding Devices”.

After you edit or create a configuration for a device, you must update the configuration on the physical FW/VPN device for the changes to take effect. For details on updating devices, see Chapter 5, “Updating Devices”.

Changes that Affect NSM-Device Connection

Certain configuration changes performed in a device update can affect the NSM connection to the device. These configuration changes include:

- Changing the connection method (Telnet or SSH) used between the NSM Device Server and the device
- Disabling the ability of the device to communicate with the NSM Device Server
- Changing the IP address of the NSM Device Server on the device
- Changing the interface on the device that is allowed to receive NSM management traffic
- Changing the VPN that is used to carry traffic between the device and the NSM Device Server
- Modifying router information on the device
- Changing policies on the device that cause NSM traffic to be dropped

The device administrator can perform some of these configuration changes using the CLI or WebUI. After the changes have been completed, you can re-import the device configuration into the Security Manager UI.

Configuring Devices in Device Manager

To configure a device that has been added and imported or modeled in Security Manager:

1. In the Navigation Tree, select Device Manager > FW/VPN Devices.
2. Double-click the device object in either the FW/VPN Device Tree or the FW/VPN Device List. (Or, either select the device object and then click the Edit icon, or right-click the device object and select Edit.)

   The Device dialog box appears. The device configuration parameters are divided by function.

3. Select a function heading in the dialog box navigation tree to see device parameters, then select the configuration parameter you want to configure.
4. Enter the configuration changes you want.
5. Click OK to save the configuration to the Security Manager GUI Server and close the Device dialog box. Click Apply to save the configuration to the GUI Server and continue entering information in the Device dialog box. Click Cancel to discard all changes and close the Device dialog box.

Device configuration parameters are described in this chapter and in the online help for the Security Manager UI.

There are two main tools you can use to simplify configuring multiple FW/VPN devices:

- **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.

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

**Templates**

Templates allow you to define a common device configuration once 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 Fields in a Template" on page 107.

The settings you make in a template are used on all devices to which you apply the template. For example, you can create a template that specifies the IP address of the NTP server to which all managed FW/VPN 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 NetScreen FW/VPN devices, from NetScreen-5XT appliances to NetScreen-5200 systems.

You can manually override any value set by a template in the configuration for a specific device. That is, if you apply a template to a device, you can change any value in the device configuration that was derived from the template.

A template can refer to other templates. Thus, you can combine multiple templates into a single template. Changes to any of the referenced templates affect the combined template.

**Creating Templates**

To create a template:

1. In the Navigation Tree, select Device Manager > FW/VPN Device Templates.
2. Click the Add icon in the Device Template Tree or the Device Template List.
The New Device Template dialog box appears. The device configuration options are divided by function. Template screens are similar in content to the device configuration screens.

3. In the Info screen, enter a name for the template you are creating.
4. Select a function heading in the dialog box navigation tree to see additional configuration parameters, then click the parameter you want to configure.

For more information about the options you can configure, see the later sections in this chapter starting with “Configuring Device Information” on page 117.

5. Enter the configuration parameters you want to set.
6. Click OK to save the configuration and close the New Device Template dialog box. Click Cancel to discard all changes and close the New Device Template dialog box.

Note the following when creating a template:

- When you edit a template, default values are not shown. Many default values depend on the ScreenOS version and device platform; templates are not specific to a specific ScreenOS version or device platform.
- Templates do not automatically include any of the entities that are predefined on devices, such as zones, interfaces, or virtual routers. If you want to create a template that refers to a specific predefined entity, you need to create the entity in the template. For example, if a template refers to the ethernet1 interface, you need to do the following:
  2. Click the Add icon in the Interface configuration screen and select Predefined Interface.
  3. Enter `ethernet1` in the Name field in the Physical Interface dialog box.

When creating a predefined entity in a template, make sure that the menu option you select when adding the entity is appropriate for the predefined entity. Choose the menu option that includes the name of the predefined entity you are creating. For example, if you are configuring the mgt zone, click the Add icon in the Zone configuration screen and select Predefined Functional Zone -- mgt/vlan, then type `mgt` in the Zone dialog box.

- Key list parameters that are derived from a template cannot be edited and are read-only in the device configuration. Key list parameters uniquely identify a configuration object in a list of similar objects. 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. Note that there can be multiple key list parameters for a configuration object. 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 and Applying a Template

The following example shows how to create a template called “DNS” that configures the IP addresses of primary and secondary DNS servers.

1. In the Navigation Tree, select Device Manager > FW/VPN Device Templates.
2. Click the Add icon in the Device Template Tree or the Device Template List. The New Device Template dialog box appears.
3. In the Info screen, enter DNS in the Name field.
4. Select Network > DNS in the dialog box navigation tree.
5. Enter the IP address of the primary and secondary DNS servers.
6. Change the default DNS refresh schedule, if necessary.
7. Click OK to save the template.

You can now use this template when configuring a single FW/VPN device. To apply the DNS template to a configuration for a device (the following steps assume that the device has previously been added):

1. In the Navigation Tree, select Device Manager > FW/VPN Devices.
2. Double-click the device to open the Device dialog box.
3. Select Info > Templates in the dialog box navigation tree.
4. Click the Edit icon in the Templates configuration screen.
The Edit Templates dialog box appears.

5. Select the DNS template.

6. Click OK in the Edit Templates dialog box.

When you view or edit a device configuration, you can see if the value in a field is derived from a template by pressing the Shift key and then moving the cursor over the field name. If the value is from a template, the following message appears: From template: template-name.
Remember that you can override any value set in a template by editing the configuration for the device; any device-specific configuration overrides a template value. To return a device-specific configuration value to the template or default value, right-click on the field name and select Revert to template/default value.

You can apply the same template to devices that are different device types and running different ScreenOS versions. In some cases, the fields or field values you specify in the template may not be appropriate for all ScreenOS versions and device types. If you apply a template that specifies a field that a device does not support, the field does not appear in the Device dialog box and is not updated to the device. If a template specifies a field that is supported by the device but the value is outside the allowed range for the device, a validation message appears in the Device dialog box.

Note that when you create and edit a template, checking may be performed on the fields and values you enter in the template and validation messages may appear. For example, a validation message may appear if you do not specify a netmask for an IP address in the same template. However, you can configure an IP address in one template and the netmask for that IP address in another template. You can safely ignore a validation message as long as the “missing” field will be derived from another template that is applied to the device or if you will manually enter in the value when configuring the device.

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 in the Security Manager UI. To change the field value on the device, you must update the device (see Chapter 5, “Updating Devices”).

When you change a template, one or more devices that use the template may become invalid. For example, the change could cause a required field to be missing or a field value to be outside the allowed range.
To modify a template, double-click the template in either the Device Template Tree or the Device Template List (or either select the template and then click the Edit icon, or right-click on the template and select Edit), and enter the configuration changes you want.

Applying Multiple Templates to a Device

A device configuration can refer to multiple templates, which are applied in a user-specified order, from the lowest priority template to the highest priority template. You can apply as many as 31 templates to a device. However, configuring certain features reduces the maximum number of templates you can apply to a device. For example, configuring a device as a vsys device or as a member of a cluster reduces the maximum number of templates by one. Each VPN you configure on a device also reduces the maximum number of templates by one. The maximum number of templates you can apply to a device also includes templates that are referenced by other templates. For example, if a device configuration refers to template A, which in turn refers to templates B and C, there are three templates applied to the device.

Note that you specify the priority in which templates are applied to a device configuration. When you apply multiple templates to a device configuration, a template can override the value of one or more fields specified in another template. When a value for a field is set in more than one template, the value in the highest-priority template takes precedence. This concept is demonstrated in the example in the next section.

Example: Creating and Applying Multiple Templates

This section shows an example of creating and applying two templates that configure different values for the same firewall SCREEN option for the untrust zone. The example demonstrates that when two templates are applied to a configuration for a NetScreen-208 device, the values in the last-applied template override the values of the previously-applied template. Finally, the example shows that you can override a template value by manually entering in a configuration value.

In this example, you first create a template that configures the Denial of Service firewall SCREEN options for the untrust zone and apply the template to the configuration for a NetScreen-208 device.

The following steps create a template “DoS” which enables several Denial of Service attack protections.

1. In the Navigation Tree, select Device Manager > FW/VPN Device Templates.
2. Click the Add icon in either the Device Template Tree or the Device Template List.
   
   The New Device Template dialog box appears.
3. In the Info screen, enter DoS in the Name field.
4. Select Network > Zone in the dialog box navigation tree.
   
   The Zone configuration screen appears.
5. Click the Add icon in the Zone configuration screen and select Predefined Security Zone.

**Note:** Since the untrust security zone is predefined for the device, you need to select the Predefined Security Zone option. You would select the Security Zone or Tunnel Zone option only if you were adding or configuring a user-defined zone.

The Predefined Zone dialog box appears.

6. Enter **untrust** in the Name field in the General Properties configuration screen.

7. Select Screen > Denial of Service Defense.

The Denial of Service Defense configuration screen appears.

8. Select the following options:
   - Ping of Death Attack Protection
   - Teardrop Attack Protection
   - Land Attack Protection
   - SYN-ACK-ACK Proxy Protection, with Threshold set to 512
   - Source IP Based Session Limit, with Threshold set to 128
   - Destination IP Based Session Limit, with Threshold set to 4000
9. Click OK in the Predefined Zone dialog box.
10. Click OK in the New Device Template dialog box.

You can apply the DoS template to any NetScreen FW/VPN device configuration, from NetScreen-5XTs to NetScreen-5400s. Remember that you can only apply a template to individual devices, not a device group.

To apply the DoS template to a device configuration for a NetScreen-208 running ScreenOS 4.0 (the following steps assume that the device has previously been added):

1. In the Navigation Tree, select Device Manager > FW/VPN Devices.
2. Double-click the NetScreen-208 device icon to open the Device dialog box.
3. Select Info > Templates in the dialog box navigation tree.
4. Click the Edit icon in the Templates configuration screen.
   The Edit Templates dialog box appears.
5. Select the DoS template.
6. Click OK in the Edit Templates dialog box.

To verify that the configuration values from the DoS template have been applied in the device configuration:

1. Select Network > Zone in the dialog box navigation tree.
2. Double-click on the untrust zone.
The untrust-Predefined Zone dialog box appears.


If you apply a template that specifies a field that a device does not support, the field does not appear in the Device dialog box and is not updated to the device. Note that in the template created earlier in this example, Denial of Service options selected included the following: Destination IP-Based Session Limit, with Threshold set to 4000. However, the device to which the template was applied is a NetScreen-208 running ScreenOS 4.0; this option is not supported on this device and does not appear in the Device dialog box for the device.

When you view or edit a device configuration, you can see if the value in a field is derived from a template by pressing the Shift key and then moving the cursor over the field name.
The next part of this example shows how to create a second template that configures a different value for a Denial of Service Defense field that was set in the DoS template. When you apply both templates to the same device configuration, you can specify which template has the higher priority. The template with the highest priority overrides the values in the lower priority template.

The following steps create a template “DoS2” which sets a threshold value of 256 for the source-based IP session limit in the untrust zone.

1. In the Navigation Tree, select Device Manager > FW/VPN Device Templates.
2. Click the Add icon in the Device Template Tree or the Device Template List.
   The New Device Template dialog box appears.
3. In the Info screen, enter DoS2 in the Name field.
4. Select Network > Zone in the dialog box navigation tree.
   The Zone configuration screen appears.
5. Click the Add icon in the Zone configuration screen and select Predefined Security Zone.
   The Predefined Zone dialog box appears.
6. Enter untrust in the Name field in the General Properties configuration screen.
7. Select Screen > Denial of Service Defense.
   The Denial of Service Defense configuration screen appears.
8. Select the Source IP Based Session Limit option, and set the Threshold to 256.
9. Click OK in the Predefined Zone dialog box.
10. Click OK in the New Device Template configuration dialog box.

To apply the DoS2 template to the configuration for the NetScreen-208:

1. In the Navigation Tree, select Device Manager > FW/VPN Devices.
2. Double-click the NetScreen-208 device icon to open the Device dialog box.
3. Select Info > Templates in the dialog box navigation tree.
4. Click the Edit icon in the Templates configuration screen to open the Edit Templates dialog box.
5. Select the DoS2 template.
6. Click OK in the Edit Templates dialog box.

At this point, note that the DoS template has the highest priority. This means that the DoS template overrides any values set by the DoS2 template. To set the DoS2 template to the highest priority:

1. Select the DoS2 template.
2. Click the down arrow icon above the list of templates. (Or press Alt-N.)

The DoS2 template now has the highest priority. The values set in the DoS2 template override values set in the DoS template.
To verify that the configuration values from the DoS and DoS2 templates have been applied in the device configuration:

1. Select Network > Zone in the Device dialog box navigation tree.
2. Double-click on the untrust zone. The untrust-Predefined Zone dialog box appears.

Note that even though 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 configuration for the device. This is because you assigned the DoS2 template a higher priority than the DoS template.

You can verify the template a field value is derived from by pressing the Shift key and then moving the cursor over the field name. For example, if you press the Shift key and then move the cursor over the Source IP Based Session Limit field name, the message “From template: DoS2” appears.
If you press the Shift key and then move the cursor over the SYN-ACK-ACK Proxy Protection field name, the message “From template: DoS” appears.

Finally, you can manually override any value set by a template. In the following example, you enter in 1000 for the threshold for the SYN-ACK-ACK Proxy Protection in the configuration for the NS-208 device. You can verify that the setting is derived from the device configuration itself and not a template by pressing the Shift key and moving the cursor over the field name. The message “From object” appears.
Device Groups

You can organize previously-created devices into user-defined groups that make it easier for you to configure and manage devices in your domain. For example, you can group devices of the same type, such as all the NetScreen-5GTs in your domain. Or, you can group devices by physical location—for example, all the NetScreen FW/VPN devices in the San Jose office. Or, you can place devices into a logical group—for example, all the NetScreen FW/VPN devices in sales offices throughout western Europe.

Groups enable you to execute certain Security Manager operations on multiple FW/VPN 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 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.

The following example shows how to create a group called “Sales”. (The devices that you add to the group must have previously been added or modeled in the domain.)

1. In the Navigation Tree, open the Device Manager and select FW/VPN Devices.
2. Click the Add icon in either the FW/VPN Device Tree or the FW/VPN Device List and select Group. The New Group dialog box appears. Note that all existing devices in the domain appear in the Non-members list.
3. Enter Sales in the Name field.
4. Select the devices in the Non-members list that are to be members of the Sales group.
5. Click Add===> to move the selected devices to the Member list.
6. Click OK.
CONFIGURING DEVICE INFORMATION

To configure a device that has been added and imported or modeled in Security Manager:

1. In the Navigation Tree, select Device Manager > FW/VPN Devices.
2. Double-click the device object in either the FW/VPN Device Tree or the FW/VPN Device List. (Or, either select the device object and then click the Edit icon, or right-click the device object and select Edit.)

   The Device dialog box appears. The device configuration options are divided by function that appear in the dialog box navigation tree.

3. Open the function heading in the dialog box navigation tree to see configuration options, then click the configuration option you want to configure.

4. Enter the changes you want in the configuration screen.

5. Click OK to save the configuration to the GUI Server and close the Device dialog box. Click Apply to save the configuration to the GUI Server and continue entering information in the Device dialog box. Click Cancel to discard all changes and close the Device dialog box.

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 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.

Configuring Startup Information

Rapid Deployment (RD) simplifies the staging and configuration of multiple FW/VPN appliances under Security Manager. With RD, the Security Manager administrator creates a configlet in the Security Manager, then sends the configlet to the user that has local access to the FW/VPN device.

For more information about RD and configlets, see Chapter 3, “Adding Devices”.

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.

To apply a template in a device configuration:

1. Click the Edit icon at the top of the Templates list.

   The Edit Templates dialog box appears.

2. Select the template to be applied. (You can also select multiple templates.)

3. Click OK in the Edit Templates dialog box.
Remember that the order in which the templates are listed is important; when a field value is set in more than one template that is applied to a device, the value in the highest-priority template takes precedence.

To change the priority of a template that you have applied to a device:
1. Select the template from the Templates list.
2. 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 “Templates” on page 103.

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 NetScreen FW/VPN 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 NetScreen FW/VPN platforms, ScreenOS versions, or license key installations.
Configuring Network Settings

The Network screens contain the options that enable the device to connect to and operate in the network. In the Device dialog box, open the Network heading in the navigation tree to see the network settings options.

This section describes configuring the following network settings for NetScreen FW/VPN devices:

- **Slot.** (This option is only available for Netscreen FW/VPN systems, such as the NS-5000 series, that contain 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.

- **Virtual Router.** A virtual router (VR) supports static routes and dynamic routing protocols. The virtual router configuration includes the configuration for dynamic routing protocols.

- **Zone.** 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.

- **Interface.** You bind interfaces to predefined or user-defined security zones or to tunnel zones to allow 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.

- **DIP Group.** You can configure a range of IP addresses from which FW/VPN device can take addresses when performing network address translation (NAT) on the source IP address of outgoing or incoming IP packets.

- **PPPoE.** (This option is only available for NetScreen FW/VPN appliances.) You can configure PPPoE to enable the FW/VPN device to connect to remote sites.

- **NACN.** (This option is only available for FW/VPN devices running ScreenOS 4.0.x.) You configure NetScreen Address Change Notification to enable the FW/VPN device to alert Security Manager of any change in the IP address assigned by a DHCP or PPPoE server.

- **Failover.** (This option is only available for some NetScreen FW/VPN appliances.) When there are both primary and backup interfaces to the Untrust zone, you can configure traffic failover traffic from the primary to the backup interface, and from the backup to the primary interface.

- **Modem.** (This option is only available for some NetScreen FW/VPN appliances.) You can connect and configure an external modem to the RS-232 serial port as a backup dialup interface for traffic to the Untrust zone.

- **DNS.** Before the NetScreen FW/VPN device can use DNS for domain name and address resolution, you must configure the addresses for the primary and secondary DNS servers.

- **Advanced.** This option contains additional network settings you can configure.
Configuring the Network Module

(This option is only available for Netscreen FW/VPN systems, such as the NS-5000 series, that contain physical slots in which you can install optional modules.) The Slot screen allows you to display or edit the type of network module installed in each available slot in the physical device.

Configuring Virtual Routers

The Virtual Router configuration screens allow you to configure static routes and dynamic routing protocols. There are two predefined virtual routers (VRs) on NetScreen FW/VPN devices:

- trust-vr, which by default contains all predefined security zones and any user-defined zones
- untrust-vr, which by default does not contain any security zones

You cannot delete the trust-vr or untrust-vr predefined virtual routers. On some NetScreen FW/VPN devices, you can create and configure additional custom virtual routers. You can configure certain fields for the predefined and custom virtual routers. For a vsys, you can select a virtual router to be the default router for the vsys.

By default, all predefined and user-defined security zones (and all interfaces bound to those security zones) are bound to the trust-vr virtual router. If you want to bind a security zone to the untrust-vr or to a custom VR, you need to first unbind all interfaces from the zone.

Adding Custom Virtual Routers

Some NetScreen FW/VPN devices allow you to create a custom virtual router. To create a virtual router:

1. Click the Add icon in the Virtual Router configuration screen.
2. Define the name of the virtual router.
3. You can configure virtual router parameters, as described in the following section.
4. Click OK.

Configuring Virtual Router Parameters

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 for the virtual router:

- General properties of the virtual router
- Access list
- Route map
- Export and import rules
Routing table

**Note:** In the routing table, you need to configure a default route for the NetScreen FW/VPN device. You should also configure a route from the device to the IP address of the Security Manager Device Manager host.

Route preferences
 Dynamic routing protocols: OSPF, RIP, and BGP

For more detailed explanations about virtual routers and dynamic routing protocols on NetScreen FW/VPN devices, see the “Dynamic Routing” volume in the NetScreen Concepts & Examples ScreenOS Reference Guide.

**Configuring Virtual Router General Properties**

You can configure the following general properties for a virtual router:

- The virtual router ID is a unique identifier used to communicate with other routing device. 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, ScreenOS automatically selects the highest IP address of the active interfaces in the VR for the router identifier.

- You can set 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 NetScreen FW/VPN 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.

- 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.

- (For the trust-vr only) You can enable or disable automatic route exporting to the untrust-vr for interfaces configured in Route mode.

- 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.

- 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.

- 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.

- (For the trust-vr only) You can direct the virtual router to use the untrust-vr as the next hop for the default route.
Chapter 4 Configuring Devices

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 allow routes for the 1.1.1.0/24 subnetwork. 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. For example, if the two previously-mentioned 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.

To create an access list:

2. Enter an Access List Number to identify the access list.
3. Click the Add icon in the Access List Entries/New dialog box. The Access List Entry dialog box appears. To configure an entry for the access list:
   a. Enter a Sequence Number.
   b. Select Permit or Deny from the Action list.
   c. Select Prefix to Filter to specify an IP address and netmask for the access list entry. Or select Default Route.
   d. Click OK. The entry you configured appears in the Access List Entries/New dialog box.
4. You can configure additional entries for the same access list, specifying a different sequence number for each entry.
5. Click OK when you are done configuring the access list.

Note that 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.

Configuring Route Maps

A route map consists of a set of statements that are applied 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.
To create a route map:

1. Click the Add icon in the Route Map configuration screen. The Route Map dialog box appears.
2. Enter a name to identify the route map.
3. Click the Add icon in the Route Map dialog box. The Route Map Entry dialog box appears. To configure an entry for the route map:
   a. Enter a Sequence Number.
   b. Configure the Match Properties to define the conditions that an incoming or outgoing route must match before further actions result.
   c. Configure the Set Properties to define the type of action that occurs when an incoming or outgoing route matches the conditions specified in the Match Properties.
   d. Click OK. The entry you configured appears in the Route Map dialog box.
4. You can configure additional entries for the same route map, specifying a different sequence number for each entry.
5. Click OK when you are done configuring the route map.

**Configuring Export and Import Rules**

If you have two virtual routers configured on a NetScreen FW/VPN device, you can allow specified routes in one VR to be learned by the other VR. To do this, you must define an export rule on the source VR that will export routes to the destination VR. When exporting routes, a virtual router allows other VRs to learn about its network. On the destination VR, you can optionally configure an import rule to control the routes that are allowed to be imported from the source VR. If there are no import rules on the destination VR, all exported routes are accepted.

The following are the basic tasks in exporting and importing routes between virtual routers:

1. On the source VR, define an export rule.
2. (Optional) On the destination VR, define an import rule. While this step is optional, an import rule allows you to further control the routes that the destination virtual router accepts from the source virtual router.

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 configure the trust-vr to automatically export all its route table entries to the untrust-vr. You can also configure a user-defined virtual router to automatically export routes to other virtual routers. Routes in networks directly connected to interfaces in NAT mode cannot be exported.

To create an export rule:

1. Click the Add icon in the Export Rules configuration screen. The Export Rule dialog box appears.
2. (Screen OS 4.0.x devices only) Select the Default Route check box to export the default route in the VR.
3. Select the Virtual Router that is to receive the route information.
4. Select the Route Map which is to be applied to the routes to be exported.
5. Select the Protocol of the routes to be exported.
6. Click OK.

To create an import rule:
1. Click the Add icon in the Import Rules configuration screen. The Import Rule dialog box appears.
2. Select the Default Route check box to import the default route into the VR.
3. Select the Virtual Router that is to send the route information.
4. Select the Route Map which is to be applied to the routes to be imported.
5. Select the Protocol of the routes to be imported.
6. Click OK.

**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 NetScreen FW/VPN device, ScreenOS 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. ScreenOS 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

For each destination network, the routing table contains the following information:
- The interface on the NetScreen FW/VPN device on which traffic for the destination network is forwarded.
- The next-hop, which can be either another virtual router on the NetScreen FW/VPN device or a gateway IP address (usually a router address).
- The protocol from which the route is derived.
- The preference is used to select the route to use when there are multiple routes to the same destination network. This value is determined by the protocol or the 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.

You can modify the preference value for each protocol or route origin on a per-virtual router basis.
• The metric can also be used to select the route to use when there are multiple routes for 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.
• The virtual system (vsys) to which this route belongs.

**Note:** In the routing table, you need to configure a default route (network address 0.0.0.0/0) for the NetScreen FW/VPN device. You should also configure a route from the device to the IP address of the Security Manager Device Manager host system.

When there are two virtual routers on a NetScreen FW/VPN device, traffic is not automatically forwarded between zones that reside in different VRs, even if there are policies that permit the 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:

1. Click the Add icon in the Destination-based Routing Table configuration screen. The Routing Table dialog box appears.
2. Enter the IP address and netmask for the destination network.
3. Select either Virtual Router or Gateway in the Next Hop list.
   - If you selected Virtual Router, select the VR that is to be the next hop for this route.
   - If you selected Gateway, 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 this route.
4. Click OK.

Some NetScreen FW/VPN devices also allow you to configure a route entry based on the source IP address of the data packet. To create a static route based on a network source:

1. Select the Enable Source-based Routing check box.
2. Click the Add icon in the Source-based Routing Table configuration screen. The Source Routing Table dialog box appears.
3. Enter the IP address and netmask for the source network.
4. Select the interface through which the next hop router is accessed in the Interface list.
5. Enter the IP address of the next hop router.
6. Enter the metric for the route.
7. Click OK.

---

NetScreen-Security Manager 2004 125
Chapter 4 Configuring Devices

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 Protocols

This sections describes the basic steps in configuring the following dynamic routing protocols:

- Open Shortest Path First (OSPF)
- Routing Information Protocol (RIP)
- Border Gateway Protocol (BGP)

OSPF

The following are the basic tasks in configuring OSPF in a VR on a NetScreen FW/VPN device:

1. Create and enable the OSPF routing instance in a VR. This step also automatically creates an OSPF backbone area, with an area ID of 0.0.0.0, which cannot be deleted.
2. (Optional) Unless all OSPF interfaces will be connected to the backbone area, you need to define a new OSPF area with its own area ID. For example, if the NetScreen FW/VPN device is to act as an ABR, you need to create a new OSPF area in addition to the backbone area. You can configure the new area as a normal, stub, or not-so-stubby area.
3. Assign one or more interfaces to each OSPF area. You must explicitly add interfaces to an OSPF area, including the backbone area.
4. Enable OSPF on each interface.

You can optionally configure other OSPF parameters, such as the following:

- Global parameters, such as virtual links, that are set at the VR level for the OSPF protocol. When you configure an OSPF parameter at the VR level, the parameter setting affects operations on all OSPF-enabled interfaces.
- Interface parameters, such as authentication, that are set on a per-interface basis for the OSPF protocol. This section describes OSPF parameters that you configure at the interface level. When you configure an OSPF parameter at the interface level, the parameter setting affects the OSPF operation only on the specific interface.
Configuring Network Settings

The following are the basic steps to configure OSPF in the Security Manager UI:

1. In the Navigation Tree, select Device Manager > FW/VPN Devices.
2. Double-click the device object in either the FW/VPN Device Tree or the FW/VPN Device List. (Or, either select the device object and then click the Edit icon, or right-click the device object and select Edit.)
   The Device dialog box appears.
4. Double-click the virtual router in which you are configuring an OSPF routing instance. The Virtual Router configuration screen appears.
5. Click Dynamic Routing Protocol in the dialog box navigation tree.
7. Select OSPF > Parameters. The Parameters configuration screen appears. In this screen, select the Enable OSPF check box.
8. If you need 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.
9. Click OK to close the Area configuration screen.
10. Click Interface in the Device dialog box navigation tree. The list of interfaces for the device appears.
11. Select the interface that is connected to OSPF peers, and click the Edit icon. The configuration screen for the interface appears.
13. Select the OSPF tab and do the following:
   a. Select the ID of the OSPF area to which the interface is bound.
   b. Select the Enable OSPF check box.
14. Click OK.

**RIP**

The following are the basic tasks in configuring RIP on a NetScreen FW/VPN device:

1. Create and enable the RIP routing instance in a virtual outer.
2. Enable RIP on interfaces that connect to other RIP routers.
You can also optionally configure other RIP parameters such as the following:

- Global parameters, such as timers and trusted RIP neighbors, that are set at the VR level for the RIP protocol. When you configure a RIP parameter at the VR level, the parameter setting affects operations on all RIP-enabled interfaces.

- Interface parameters, such as neighbor 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.

The following are the basic steps to configure RIP in the Security Manager UI:

1. In the Navigation Tree, select Device Manager > FW/VPN Devices.
2. Double-click the device object in either the FW/VPN Device Tree or the FW/VPN Device List. (Or, either select the device object and then click the Edit icon, or right-click the device object and select Edit.)

   The Device dialog box appears.
4. Double-click the virtual router in which you are configuring a RIP routing instance. The Virtual Router configuration screen appears.
5. Click Dynamic Routing Protocol in the dialog box navigation tree.
7. Select RIP > Parameters from the dialog box navigation tree. The Parameters configuration screen appears. In this screen, select the Enable check box.
8. Click OK to close the Parameters configuration screen.
9. Click Interface in the Device dialog box navigation tree. The list of interfaces for the device appears.
10. Select the interface that is connected to the RIP peer, and click the Edit icon. The configuration screen for the interface appears.
12. Select the RIP tab and do the following:
   a. Select the Bind Interface to RIP check box.
   b. Select the Enable RIP check box.
13. Click OK.
**BGP**

The following are the basic tasks in configuring BGP in a virtual router on a NetScreen FW/VPN device:

1. 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.
2. Enable and configure the BGP peer.
3. 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 will either be sent to or received from the peer, which causes the connection to fail or close.

You can configure parameters for individual peer addresses. You can also assign peers to a peer-group, which then allows you configure parameters for the peer-group as a whole. Note that you cannot assign IBGP and EBGP peers to the same peer-group.

The following are the basic steps to configure BGP in the Security Manager UI:

1. In the Navigation Tree, select Device Manager > FW/VPN Devices.
2. Double-click the device object in either the FW/VPN Device Tree or the FW/VPN Device List. (Or, either select the device object and then click the Edit icon, or right-click the device object and select Edit.)
   
   The Device dialog box appears.
4. Double-click the virtual router in which you are configuring a BGP routing instance. The Virtual Router configuration screen appears.
5. Click Dynamic Routing Protocol in the dialog box navigation tree.
7. Select BGP > Parameters from the dialog box navigation tree. The Parameters configuration screen appears. In this screen, do the following:
   a. Select the Enable BGP check box.
   b. Enter an AS Number.
8. Select BGP > Neighbors from the dialog box navigation tree. The Neighbors configuration screen appears. In this screen, do the following:
   a. Click the Add icon.
   b. Select Peer Enabled.
   c. Enter in the BGP peer information.
Chapter 4 Configuring Devices

9. Click OK to close the Neighbors configuration screen.
10. Click Interface in the Device dialog box navigation tree. The list of interfaces for the device appears.
11. Select the interface that is connected to the BGP peer, and click the Edit icon. The configuration screen for the interface appears.
13. Select the Enable BGP check box under the BGP tab.
14. Click OK.

Configuring Zones

The Zone configuration screen allows you to 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.

Adding a Security or Tunnel Zone

To create a security or tunnel zone:

1. Determine the zone type:
   - A layer 3 zone is a zone to which you bind NAT or Route mode interfaces
   - A layer 2 zone is a zone to which you bind Transparent mode interfaces

   **Note:** When you add a device, you can specify if the device is to operate in Transparent mode. If you chose Transparent mode for the device, the L2 zone names appear in the Security Manager UI without the “V1-” prefix. When you update the configuration on the device from the UI, the correct L2 zone names are configured.

   - A tunnel zone is a zone to which you bind a carrier zone

2. Click the Add icon in the Zone configuration screen, and select either Security Zone or Tunnel Zone.
3. 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.

4. Click OK.
Configuring Zone Parameters

To configure a zone, double-click the zone in the Zone configuration screen (or, either select the interface and then click the Edit icon, or right-click the Zone and select Edit). For security zones, you can configure the following:

- Enable predefined SCREEN options that detect and block various kinds of traffic that the FW/VPN device determines to be potentially harmful.
- Enable malicious URL protection that directs the FW/VPN device to drop incoming HTTP packets that reference URLs that match certain user-defined patterns.
- Block traffic between hosts within the security zone.
- Enable reassembly of fragmented IP packets and TCP segments for application layer gateway (ALG) filtering.
- Direct the FW/VPN device to send back a TCP segment with the RESET flag set to 1 when a TCP segment with a flag other than SYN is received.

For more detailed information about zones on NetScreen FW/VPN devices, see the “Fundamentals” volume in the NetScreen Concepts & Examples ScreenOS Reference Guide.

Configuring Interfaces

The Interface screen shows the physical interfaces available on the NetScreen FW/VPN device. Some NetScreen systems 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.

Adding Interfaces

You can add the following interfaces on a NetScreen FW/VPN device:

- An aggregate interface is the accumulation of two or more physical interface which share the traffic load to a single IP address. This type of interface is only supported on certain NetScreen FW/VPN systems.
- A loopback interface is a logical interface that emulates a physical interface and is always in the up state.
- Virtual security interfaces (VSIs) are the virtual interfaces that two NetScreen FW/VPN devices share when forming a virtual security device (VSD) in a high availability cluster.
- A 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.
A subinterface is a logical division of a physical interface. A subinterface borrows the bandwidth it needs from the physical interface.

A tunnel interface acts as a doorway to a VPN tunnel. Traffic enters and exits a VPN tunnel via a tunnel interface.

**Configuring Interface Parameters**

From the Interface screen, 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:

- General Properties. You can set the following:
  - IP address of the interface
  - Zone to which the interface is bound
  - Loopback interface group to which the interface belongs
  - Redundant interface group to which the interface belongs
  - Mode of the interface (NAT or route)
  - Enable management services

- Advanced Properties. You can set attributes of the physical link for the interface.

- DHCP. The Dynamic Host Configuration Protocol (DHCP) automatically assigns TCP/IP settings for the hosts on the network. Different NetScreen FW/VPN 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.

- Protocol. You can enable and configure dynamic routing protocol operation on the 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.

- Track IP. You can enable the NetScreen FW/VPN device to monitor the reachability of certain IP addresses through the interface to determine interface failure. For each IP address to be tracked, you 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.

- NAT. You can configure the following address translation methods on the NetScreen FW/VPN device: Mapped IP (MIP), dynamic IP (DIP), or virtual IP (VIP) settings.

For more detailed explanations about interfaces on NetScreen FW/VPN devices, see the “Fundamentals” volume in the NetScreen Concepts & Examples ScreenOS Reference Guide.

Configuring DIP Groups

The DIP Group option allows you to combine two DIP pools into one DIP group. This enables you to define a policy to perform NAT using the DIP group for two NetScreen FW/VPN devices that are in an active/active NRSP configuration. Otherwise, the NetScreen FW/VPN device that acts as the backup of a VSD group would not be able to use a DIP pool located on the VSI of the master of the VSD group.

To configure a DIP pool for an interface:

1. Select Network > Interface in the Device dialog box navigation tree.
2. Double-click the interface for which you are configuring the DIP pool.
   The Interface configuration screen appears.
3. Select NAT > DIP in the Device dialog box navigation tree.
   The Dynamic IP dialog box appears.
4. Configure the DIP pool.
5. Click OK to close the Dynamic IP dialog box.

To create a DIP group:

1. Select Network > DIP Group in the Device dialog box navigation tree.
2. Click the Add icon in the DIP Group configuration screen.
   The Dynamic IP dialog box appears.
3. Select the ID number for the DIP group.
4. Select the DIP pool members for the group.
5. Click OK to close the Dynamic IP dialog box.

For more detailed explanation about DIP groups on NetScreen FW/VPN devices, see the “Fundamentals” volume in the NetScreen Concepts & Examples ScreenOS Reference Guide.

Configuring PPPoE

The PPPoE option allows you to configure PPPoE operations. Some NetScreen FW/VPN devices support PPPoE, allowing them to operate compatibly on DSL, Ethernet Direct, and cable networks run by ISPs that use PPPoE for their clients’ Internet access.
You can configure a specific instance of PPPoE and assign a username and password and other parameters for that instance. For NetScreen FW/VPN devices running ScreenOS 4.0.0, you can only enable PPPoE on a single interface bound to the Untrust zone. For NetScreen FW/VPN devices running ScreenOS 5.0.0, you can enable PPPoE on multiple interfaces in any zone at the same time.

**Note:** Some ISPs use DHCP for their clients' Internet access. To configure DHCP on an interface, see “Configuring Interface Parameters” on page 132.

To add a PPPoE instance:

1. Click the Add icon in the PPPoE configuration screen. The PPPoE Instance dialog box appears.
2. Enter the name for the PPPoE instance.
3. Select the interface to which this PPPoE instance applies.
4. Enter the username and password for the instance.
5. Configure any other PPPoE parameters, as needed.
6. Click OK to close the PPPoE Instance dialog box.

For more detailed explanation about PPPoE or DHCP on NetScreen FW/VPN devices, see the “Fundamentals” volume in the NetScreen Concepts & Examples ScreenOS Reference Guide.

**Configuring NACN**

The NACN option allows you to configure NetScreen Address Change Notification (NACN). NACN is only available on FW/VPN devices running ScreenOS 4.0.x. Before the NetScreen-Security Manager can contact a NetScreen FW/VPN device, it must have the current IP address of the device interface. This is relatively easy when the NetScreen FW/VPN device has a static IP address on its interface. However, an interface on a NetScreen FW/VPN device can have a dynamically assigned IP address, using either PPPoE or DHCP. In these cases, the NetScreen FW/VPN device uses NACN to monitor a specific interface and then register with Security Manager the IP address of the interface whenever it changes. This prevents interruption of communication between Security Manager and the NetScreen FW/VPN device.

For more detailed explanation about NACN on NetScreen FW/VPN devices, see the “Administration” volume in the NetScreen Concepts & Examples ScreenOS Reference Guide for ScreenOS 4.0.0.
Configuring Interface Failover

(This option is only available for some NetScreen FW/VPN appliances.) The Failover option allows you to configure the FW/VPN 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 NetScreen FW/VPN 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 NetScreen FW/VPN devices, see the “High Availability” volume in the NetScreen Concepts & Examples ScreenOS Reference Guide for ScreenOS 5.0.0 or the New Features Guide for ScreenOS 4.0.0-DIAL2.

Configuring a Modem Connection

(This option is only available for some NetScreen FW/VPN appliances.) The Modem option allows you to configure the NetScreen FW/VPN device for operation with an external modem. You can connect an external modem to the RS-232 serial port on certain NetScreen FW/VPN devices to allow 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) is the maximum baud rate for the serial link (the default rate is 115200 bps).
- Timeout is 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 is 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 is 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 NetScreen FW/VPN 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 will dial the ISP with the next highest priority number, and so on, until there are no more ISP configurations.

To create the settings for an 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 NetScreen FW/VPN devices, see the “High Availability” volume in the NetScreen Concepts & Examples ScreenOS Reference Guide for ScreenOS 5.0.0 or the New Features Guide for ScreenOS 4.0.0-DIAL2.

Configuring DNS

The DNS option allows you to configure DNS server information. Before the FW/VPN device can use DNS for domain name/address resolution, you must configure the address for the primary DNS server the device should use.

The NetScreen FW/VPN device refreshes all the entries in its DNS table by checking them with a specified DNS server at the following times:

- After an HA failover occurs
- At a regularly scheduled time of day and at regularly scheduled intervals

For more detailed explanation about configuring DNS on NetScreen FW/VPN devices, see the “Fundamentals” volume in the NetScreen Concepts & Examples ScreenOS Reference Guide.

Configuring Advanced Network Settings

The Advanced screens allow you to configure the following network settings:

- ARP cache entries
- VIP options
- DIP options

Configuring ARP Cache Entries

The ARP option allows you 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 NetScreen FW/VPN devices, see the arp commands in the NetScreen CLI Reference Guide.
Chapter 4 Configuring Devices

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 NetScreen FW/VPN 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 NetScreen FW/VPN device to forward from the VIP to the IP address of the host.

The VIP Options configuration screen allows you 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 NetScreen FW/VPN device.

For more detailed explanation about configuring VIPs on NetScreen FW/VPN devices, see the “Fundamentals” volume in the NetScreen Concepts & Examples ScreenOS Reference Guide.

Configuring DIP Options

The DIP Options allow you to set DIP translation operation. When DIP is configured on an interface, the NetScreen FW/VPN 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. You can ensure that the device assigns the same IP address from a DIP pool to a host for multiple concurrent sessions by selecting the DIP Translation Stickiness check box.

For more detailed explanation about configuring DIP options on NetScreen FW/VPN devices, see the “Fundamentals” volume in the NetScreen Concepts & Examples ScreenOS Reference Guide.
CONFIGURING DEVICE ADMINISTRATION

The Device Admin screens contain administrative options for the device. In the Device dialog box, open the Device Admin heading to see configuration options.

This section describes configuring the following device administration options for NetScreen FW/VPN devices:

- Date/time
- Management
- Banners
- Default servers

For more detailed explanation about configuring device administration on NetScreen FW/VPN devices, see the “Fundamentals” and “Administration” volumes in the NetScreen Concepts & Examples ScreenOS Reference Guide.

Configuring Date and Time Settings

The Date/Time option allows you to configure date and time synchronization on NetScreen FW/VPN devices. The date and time setting on your device affects the set up of VPN tunnels and the timing of schedules. To ensure that the NetScreen FW/VPN device always maintains the right time, it can use NTP (Network Time Protocol) to synchronize its system clock with that of an NTP server over the Internet. You can configure the NetScreen FW/VPN device to perform this synchronization automatically at time intervals that you specify. You can configure up to three NTP servers (one primary and two backups) from which the NetScreen FW/VPN device can regularly update its system clock.

In the Security Manager UI, you can direct the NetScreen FW/VPN device to immediately synchronize its system clock with an NTP server. For more information, see Chapter 6, “Managing Devices”.

Configuring Management

The Management option allows you to configure the following device management options:

- The idle time for WebUI management
- The default server for authenticating admin users
- The banners displayed at the top of a Telnet, SSH, or console session when an admin user logs into the NetScreen FW/VPN device
- Enabling SSL management: select the certification, port, cipher, and authentication you want to use
Configuring Banners

The Banners option allows you to configure the following messages:

- For Telnet, FTP, or HTTP users:
  - message that appears when user tries to log on to the device
  - message that appears when the user is successfully authenticated and a connection established
  - message that appears when the authentication fails or the user is unauthorized to access the device
- The message that appears at the top of a Web browser screen after an auth user has successfully logged on to a WebAuth address

All of the banners have default messages. You can customize the messages that appear on the banners to better suit the network environment in which you use the NetScreen FW/VPN device.

To customize a banner message:

1. Click the tab for the type of banner you want to customize in the Banners configuration screen.
2. Edit the banner message.
3. Click OK.

Configuring Default Servers

The Default servers option allows you to select a default authentication server and a default Web authentication server. You configure authentication servers as part of domain administration (see Chapter 2, "Configuring Role-Based Administration (RBA)").

All NetScreen FW/VPN devices support a built-in user database for authentication. When you define a user on the NetScreen FW/VPN device, the NetScreen FW/VPN device enters the user name and password in its local database. The local database is the default authentication server (auth server) for all types of authentication.

Before sending traffic to an intended destination, an auth user initiates an HTTP session to the IP address hosting the WebAuth feature on the NetScreen FW/VPN device and authenticates himself or herself. After the NetScreen FW/VPN device authenticates the user, he or she can then send traffic to the destination as permitted by a policy requiring authentication via WebAuth. You can select a default WebAuth server from a list of servers that you previously configured.

By default, the local database authentication timeout for both admins and auth users is 10 minutes. You can change this timeout.
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 describes configuring the following reporting options for NetScreen FW/VPN devices:

- General
- Email
- NSM
- SNMP
- Syslog
- Webtrends

For more detailed explanation about configuring reporting on NetScreen FW/VPN devices, see the "Administration" volume in the NetScreen Concepts & Examples ScreenOS Reference Guide.

Configuring General Reporting Options

The General option allows you to select the severity levels of the messages you want to log and where you want those messages sent. Each system event on a NetScreen FW/VPN device is assigned a level of severity. You can configure your NetScreen FW/VPN device to send messages to specific destinations to communicate events of a certain level of severity. By default, packets that are dropped on the NetScreen FW/VPN 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.

To configure log settings:

1. Click the tab for the type of log you want to configure in the General configuration screen.
2. Select or deselect the options you want.
3. Click OK.

Configuring Email Notification

The Email option allows you to configure the NetScreen FW/VPN device to send messages via email whenever a system event of a certain severity level occurs. To configure email notification, you need to specify the SMTP mail server and up to two destination email addresses.

To configure email notification:

1. Select the Enable Notification for Alarms check box.
2. If you want to send traffic log messages via email, select the Include Traffic Log check box.
3. Enter the name of the SMTP mail server and up to two email addresses.
4. Click OK.

Configuring NSM Reporting

The NSM option allows you to enable the NetScreen FW/VPN device to report specified events to Security Manager. You configure the primary IP address of the Security Manager Device Server and select the categories of events that are tracked on the FW/VPN device and reported to Security Manager. You can also set the interval at which the Security Manager Device Server polls for policy statistics and protocol distribution events.

Configuring SNMP Reporting

The SNMP option allows you to configure the Simple Network Management Protocol (SNMP) agent for the NetScreen FW/VPN device. The SNMP agent provides network administrators with a way to view statistical data about the network and the devices on it, and to receive notification of system events of interest.

To configure the SNMP agent on the NetScreen FW/VPN device, you set the following:

- Contact information in case the SNMP community member needs to contact someone about the device
- Physical location of the device
- Port numbers that the device uses to listen and transmit SNMP traps
- Enable the sending of traps whenever someone illegally attempts an SNMP connection to the device
- Enable the sending of SNMP messages through a VPN tunnel

You also must enable SNMP manageability on the interface through which the SNMP manager communicates with the SNMP agent in the FW/VPN device.

Creating SNMP Communities

To configure the SNMP agent on the NetScreen FW/VPN device, you must create communities, define 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:

1. Click the Add icon in the Community Settings portion of the SNMP configuration screen. The SNMP Community dialog box appears.
2. Specify the community name, whether the community has read-write or read-only privileges, whether the community receives traps or not, and whether the community supports SNMPv1, SNMPv2c, or both SNMP versions, as required by the SNMP management stations. (For backward compatibility with earlier ScreenOS releases that only support SNMPv1, NetScreen FW/VPN devices support SNMPv1 by default.)
3. Define the host(s) associated with the community:
   a. Click the Add icon to define the host associated with the community.
   b. 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.
   c. Click OK.
4. Click OK in the SNMP Community dialog box.

### Configuring Syslog Reporting

The Syslog option allows you to configure syslog reporting. A NetScreen FW/VPN 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 NetScreen FW/VPN device is to use 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 NetScreen FW/VPN device sends syslog messages.
3. For each syslog host, you specify the following:
   - Whether the NetScreen FW/VPN 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.

### Configuring Webtrends Reporting

The Webtrends option allows you to configure the NetScreen FW/VPN device to send syslog reports to a Webtrends Syslog host. Webtrends offers a product called the Webtrends Firewall Suite that allows you to customize syslog reports to display the information you want in a graphical format.
To configure the NetScreen FW/VPN 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.
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 NetScreen FW/VPN devices:

- Antivirus (AV)
- URL filtering
- Deep inspection
- Attack database

Configuring Antivirus (AV) Settings

(This option is only available on some NetScreen FW/VPN devices.) The antivirus (AV) option allows you to configure AV scanning. NetScreen FW/VPN devices provide embedded AV scanning or external AV scanning in conjunction with Trend Micro. With embedded AV scanning, the AV scanner is inside the device; embedded AV scanning is only supported on some NetScreen FW/VPN devices. With external AV scanning, the AV scanner is a separate device to which the NetScreen FW/VPN device forwards traffic that requires scanning.

To configure AV settings:

1. Click the tab for the type of settings you want to configure in the AntiVirus configuration screen:
   - AV Scanner Settings configures parameters for external AV scanners
   - AV Scan Manager Settings configures parameters for the internal AV scanner
   - AV HTTP Webmail Settings configures the device for WebMail scanning

   For descriptions of these settings, see the following sections.

2. Specify the options you want.

3. Click OK.

Configuring External AV Scanners

The AV Scanner Settings tab allows you to configure the following:

- Fail Mode Traffic Permit. You can direct the device to pass traffic if the device loses connectivity with the AV scanner.
- Maximum AV resources allowed per AV client. You can set the maximum percentage of AV resources allowed per AV client.
- HTTP Settings. You can direct the device to use the HTTP keep-alive connection option.
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

The AV Scan Manager Settings tab allows you to configure the following:

- **Pattern Server URL.** You specify the URL address of the server from which the device retrieves pattern file updates.
- **Update Interval.** You can specify the interval at which the device starts an automatic pattern update.

**Note:** You can direct a NetScreen FW/VPN device to immediately contact the pattern server and update its pattern file. To do this, right-click on the device object in the FW/VPN Device Tree or FW/VPN Device List tab in the Device Manager, and select AV Scan Manager > Update Pattern. (You can modify the pattern server URL and update interface if necessary.) Click OK.

- **Maximum Decompression Level.** You can specify the maximum number of layers of nested compressed files that the scanner decompresses before executing a virus scan.
- **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, or POP3) that are to be examined for virus patterns and the number of seconds allowed for a scan.

Configuring Webmail Scanning

The AV HTTP Webmail Settings tab allows you to enable virus scanning for webmail.

To specify a URL pattern:

1. Click the Add icon in the AV HTTP Webmail Settings tab in the AntiVirus (AV) configuration screen.
   
   The URL Pattern dialog box appears.

2. Enter the following information:
   - User-defined name for the pattern
   - The download URL path for the webmail
   - URL arguments, which begin with “?”
   - The host name included in the URL

3. Click OK to close the URL Pattern dialog box.
For more detailed explanations of AV settings, see the “Attack Detection and Defense Mechanisms” volume in the NetScreen Concepts & Examples ScreenOS Reference Guide for ScreenOS 5.0.0.

Configuring URL Filtering

The URL Filtering option allows you to configure URL filtering using the Websense Enterprise Engine, which enables you to block or permit access to different sites based on their URLs, domain names, and IP addresses. With the Websense API built directly into the NetScreen firewall, the NetScreen FW/VPN device creates a direct link to a Websense URL-blocking server.

To configure URL filtering with a Websense URL-blocking server, you enable URL filtering and define the following:

- Interface from which the NetScreen FW/VPN device initiates URL filter requests to the Websense server sent through a VPN tunnel
- Name and port for the Websense server
- Whether you want the device to block or permit all HTTP requests if connectivity to the Websense server is lost

You can also configure the timeout for receiving responses from the server and the message that is returned to the user when the user tries to access a blocked site.

For more detailed explanations of URL filtering, see the “Fundamentals” volume in the NetScreen Concepts & Examples ScreenOS Reference Guide for ScreenOS 4.0.0 or the “Attack Detection and Defense Mechanisms” volume in the NetScreen Concepts & Examples ScreenOS Reference Guide for ScreenOS 5.0.0.

Configuring Deep Inspection

(This option is only available on some NetScreen FW/VPN devices.) Deep Inspection (DI) is a mechanism for filtering the traffic permitted by the NetScreen firewall. You can enable Deep Inspection in policies to examine permitted traffic and take action if the DI module in ScreenOS finds attack signatures or protocol anomalies. Protocol anomaly detection is particularly useful for catching new attacks or those attacks that cannot be defined by a textual pattern. Attack objects that search for protocol anomalies detect traffic that deviates from the standards defined in RFCs and common RFC extensions. NetScreen supports protocol anomaly attack objects for the following protocols:

- DNS
- POP3
- SMTP
- IMAP
- FTP
- HTTP
Chapter 4 Configuring Devices

The Deep Inspection configuration screen allows you to modify the default settings defined in RFCs and RFC extensions for these protocols.

You can also enable the validation of all TCP packets for TCP checksum by clicking the Enable TCP Checksum check box.

For more detailed explanation of Deep Inspection, see the “Attack Detection and Defense Mechanisms” volume in the NetScreen Concepts & Examples ScreenOS Reference Guide for ScreenOS 5.0.0.

Configuring the Attack Database

(This option is only available on some NetScreen FW/VPN devices.) The Attack Database option allows you to configure an attack object database which contains all the predefined attack objects, organized into attack object groups by protocol and severity level. NetScreen stores the attack object database on a server at https://services.netscreen.com/restricted/sigupdates. To use the predefined attack objects, you must download the database from this server, load it on your NetScreen FW/VPN device, and then reference specific attack object groups in policies.

To gain access to the attack object database server, you must first obtain an attack object update subscription for your NetScreen FW/VPN device. To obtain a subscription for a device using the Security Manager UI, see Chapter 6, “Managing Devices”.

To configure the attack object database, specify the following:

- URL of the attack object database server
- The mode for checking and updating the database:
  - Notification checks the server at user-defined times and notifies you if the database on the server is more recent than the database on the NetScreen FW/VPN device
  - Update checks the server at user-defined times and automatically updates the database on the device if the database on the server is more recent
- Schedule (daily, weekly, or monthly) on which the NetScreen FW/VPN device checks the attack object database server

From the Security Manager UI, you can direct the NetScreen FW/VPN device to update its attack object database immediately. See Chapter 6, “Managing Devices”.

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 for ScreenOS 5.0.0.
Configuring Advanced Device Settings

The Advanced screens contain advanced options that you can set for the device. In the Device dialog box, open the Advanced heading to see configuration options.

This section describes configuring the following advanced options for NetScreen FW/VPN devices:

- Pre-defined service timeout
- SIP settings
- Traffic shaping
- Packet flow
- TFTP/FTP
- Host/domain name

Configuring Timeouts for Predefined Services

The Predefined Service Timeout option allows you 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 NetScreen FW/VPN devices, see the “Fundamentals” volume in the NetScreen Concepts & Examples ScreenOS Reference Guide.

Configuring SIP Settings

The SIP Settings option allows you to configure Session Initiation Protocol (SIP) as a service on the NetScreen FW/VPN device. The device can then screen SIP traffic, allowing and denying it based on a policy that you configure. SIP is a predefined service in ScreenOS and uses port 5060 as the destination port. Note that NetScreen FW/VPN devices currently do not support NAT (network address translation) with SIP.
Essentially, 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 a client to a server and responses to the requests from a server to a client 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 NetScreen FW/VPN 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.

There are two types of inactivity timeouts that you can configure 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 NetScreen FW/VPN device removes all sessions for this call from its table, thus terminating the call.

For more detailed explanation about configuring SIP on NetScreen FW/VPN devices, see the “Fundamentals” volume in the NetScreen Concepts & Examples ScreenOS Reference Guide.

### Configuring Traffic Shaping

The Traffic Shaping option allows you to configure traffic shaping parameters. Traffic shaping is the allocation of network bandwidth at a guaranteed Quality of Service (QoS) to every user and application on an interface. You can use a NetScreen FW/VPN device to shape traffic by creating policies and by applying traffic shaping to each class of traffic going through the device.

You can configure the following traffic shaping parameters:

- The mapping 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 NetScreen FW/VPN device maps to 111 in the IP precedence field. The lowest priority (priority 7) maps to 000 in the IP precedence field.
- The traffic shaping mode is automatically determined by the device, but you can set it to on or off.
You can only apply traffic shaping to policies 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 information about using traffic shaping with a policy, see Chapter 8, “Configuring Firewall Policies”.

For more detailed explanation about configuring traffic shaping on NetScreen FW/VPN devices, see the “Fundamentals” volume in the NetScreen Concepts & Examples ScreenOS Reference Guide.

Configuring Packet Flow

The Packet Flow option allows you to configure the NetScreen FW/VPN device to regulate packet flow. You can set the following:

- Enable or disable DNS replies when there is no matching DNS request
- Pass or block packets containing destination MAC addresses that are not in the MAC learning table
- Set or display the initial session timeout values
- Control or prevent packet fragmentation
- Age or timeout sessions in the session table

For more detailed explanation about configuring packet flow on NetScreen FW/VPN devices, see the *flow* commands in the NetScreen CLI Reference Guide.

Configuring TFTP/FTP Server Operation

The TFTP/FTP option allows you to configure a NetScreen FW/VPN device to allow TFTP or FTP servers to save or import external files. These files can contain configuration settings, software versions, public keys, error messages, certificates, and other items.

For TFTP servers, you can specify the following:

- Source interface
- Number of times that the server can retry a TFTP communication before the NetScreen FW/VPN device ends the attempt
- Timeout (in seconds) before the device terminates an inactive TFTP connection.

You can also allow FTP servers to dynamically negotiate a data port other than port 20.

For more detailed explanation about configuring TFTP or FTP servers for NetScreen FW/VPN devices, see the *ip* commands in the NetScreen CLI Reference Guide.

Configuring Host and Domain Name

The Host/Domain Name option allows you to configure a host and domain name for the NetScreen FW/VPN device. The host name is a character string that identifies the device. The host name, combined with a domain name, allows other devices to access the NetScreen FW/VPN 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 NetScreen FW/VPN devices, see the `hostname` and `domain` commands in the NetScreen CLI Reference Guide.
Configuring L2TP/XAuth/Local Users

The L2TP/XAuth/Local User option allows you to configure users for authentication or for VPN access. You can group VPN users to reduce the number of policies required to support dialup users. If you configure an L2TP or XAuth user, you need to specify L2TP or XAuth remote settings.

To configure an L2TP or XAuth user for authentication:

1. Click the Add icon in the L2TP/XAuth/Local User configuration screen. The L2TP/XAuth User Settings dialog box appears.
2. Select the user name from the User scrolling list.
3. Select the L2TP or XAuth settings from the Remote Setting scrolling list.
4. Select the L2TP pool from the IP Pool scrolling list or enter in an IP address in the Static IP field.
5. Click OK.

For more detailed explanation about configuring authentication users on NetScreen FW/VPN devices, see the "Fundamentals" volume in the NetScreen Concepts & Examples ScreenOS Reference Guide.
Chapter 4 Configuring Devices

**CONFIGURING VSYS**

After you create a vsys, you need to perform other configurations to make it a functional vsys. You need to configure interfaces or subinterfaces for the vsys, and possibly shared virtual routers and shared security zones. After completing these configurations, you can then exit the virtual system and allow the domain administrator to log into the virtual system and begin configuring addresses, users, services, VPNs, and policies.

For more detailed explanations of vsys, see the “Virtual Systems” volume in the NetScreen Concepts & Examples ScreenOS Reference Guide.

To configure a vsys:

1. In the Device Manager, double-click the vsys in either the FW/VPN Device Tree or the FW/VPN Device List. (Or, either select the vsys and click the Edit icon, or right-click on the vsys and select Edit.)
   
The Virtual System dialog box appears. The Virtual System dialog box is similar to the Device dialog box, but with fewer options.

2. Select the option you want to configure in the Virtual System dialog box navigation tree.

**Configuring Virtual Routers for a vsys**

When you create a vsys object, the vsys automatically has the following virtual routers available for its use:

- All shared root-level virtual routers
- Its own non-sharable virtual router named vsys_name-vr

You can configure any shared root-level virtual router or the vsys-level virtual router as the default virtual router for the vsys. You can define any root-level VR as sharable. If you configure a root-level virtual router to be shared, you cannot unshare it without removing all vsys first.

**Configuring Zones for a vsys**

Each virtual system (vsys) is a unique security domain and can share security zones with the root system and have its own security zones. When a root-level admin creates a vsys object, the following zones are automatically inherited or created:

- All shared zones (inherited from the root system)
- Shared Null zone (inherited from the root system)
- Trust-vsys_name zone
- Untrust-Tun-vsys_name zone
- Global-vsys_name zone

1. A shared zone must in a shared virtual router, although a zone in a shared VR can be either shared or unshared.
Each vsys can also support extra 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 vsys.

IP-based traffic classification allows you to use virtual systems without VLANs. The NetScreen FW/VPN device uses IP addresses to sort traffic, associating a subnet or range of IP addresses with either the root or a specific vsys. To designate a subnet or range of IP addresses to the root system or to a previously-created vsys, you must enable IP classification at the root level on the shared zone.

**Configuring Interfaces for a vsys**

You can configure any of the following types of interfaces for a vsys:

- Dedicated physical interface
- Subinterface, with VLAN tagging to determine the vsys that inbound or outbound traffic belongs
- Shared interface with the root system

A shared interface is an interface that can be shared with the root system or another vsys. Any interface you bind to a shared zone is shared. By default, the predefined untrust-vr is a shared VR, and the predefined Untrust zone is a shared zone. Therefore, a vsys can share any root-level physical interface, subinterface, redundant interface, or aggregate interface bound to the Untrust zone.

A 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. If you import a physical or aggregate interface into a vsys and bind it to either a shared zone or the Trust-vsys_name zone, the interface becomes a dedicated interface for the vsys. When you configure a subinterface in a vsys, it belongs to that vsys.

**Viewing vsys on the Root Device**

Selecting the VSYS option on the Device dialog box navigation tree for the root device allows you to view the vsys that are currently created on the device.

---

1. A shared interface must be configured at the root level and bound to a shared zone in a shared virtual router.
To authenticate external devices, use a Group IKE ID to authenticate multiple RAS users, or provide additional authentication for the FW/VPN devices in your VPN, you must obtain and install a digital certificate on each FW/VPN device that is a 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:

- **A local certificate** for each FW/VPN 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.

If you have imported a NetScreen FW/VPN device that already has a local certificate, CA, and CRL, these objects are automatically imported when you add that device to the Security Manager system. However, to reuse the CA and CRL objects in other NetScreen FW/VPN devices, you must load the CA and CRL file directly into the management system. For details, see “Using Imported Certificates” on page 160.

### Configuring a Local Certificate

A local certificate validates the identity of the FW/VPN 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 (a .cer file).

You must install this local certificate file on the managed device using 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.
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 NetScreen FW/VPN device.
- **Phone.** Enter the telephone number of the certificate requestor.
- **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 NetScreen FW/VPN device.
- **Key Pair Type.** Select RSA or DSA encryption.
- **Key Pair Length.** Select the key length: 512, 786, 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.
- **Automatically Enroll.** Enable 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 using SCEP, the device automatically sends its public key to the CA directly. Close the job window.
- If you are obtaining the local certificate manually, you need this information 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.

Obtaining and Installing the Certificate

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, load the certificate into the management system using the Security Manager UI, and install the certificate 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.

### 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 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.

### 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 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.
Configuring CA Certificates

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 certificate, then use this file to create a Certificate Authority object.

You must install this CA certificate on the managed device using 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 Chapter 7, “Configuring Objects”.

The following sections detail how to add a CA certificate to a device using SCEP or manually.

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.

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.

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.
Chapter 4 Configuring Devices

Configuring CRLs

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 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 Chapter 7, “Configuring Objects”.

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.
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 have imported a NetScreen FW/VPN device that already has a local certificate, CA, and CRL, these objects are automatically imported when you add that device to the Security Manager system. Imported objects use the default name of <CN>_<timestamp>.

However, to reuse the CA and CRL objects in other NetScreen FW/VPN 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 FW/VPN 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.
- **Enable raw common name.**

### 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.**
  - 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.** 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.
  - **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.**
  - **No revoke status check for CA delegated signing cert.**
  - **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 NetScreen FW/VPN 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 FW/VPN device identity to the CA.
- **CA Certificate Authentication.**
  - **Auto.**
  - **Manual.**
- **Polling Interval.**
  - **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 a group of NetScreen FW/VPN devices that enforce the same security policy and share the same configuration settings. When you assign a FW/VPN 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 forth).

Before two NetScreen FW/VPN devices can provide redundant network connectivity, you must group them in the same NSRP cluster by assigning a cluster ID between 1 and 7. When you add a NetScreen FW/VPN device into an NSRP cluster, the device automatically becomes a member of Virtual Security Device (VSD) group 0 and all its interfaces become Virtual Security Interfaces (VSIs) for VSD group 0.

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 for ScreenOS 5.0.0.

**Creating an NSRP Cluster**

To create an NSRP cluster:

1. In the Device Manager, click the Add icon in either the FW/VPN Device Tree or the FW/VPN Device List, and select Cluster.
2. In the New Cluster dialog box, enter a name for the cluster.
3. Select the device model in the Physical Choice drop-down list box, and select the ScreenOS version for the OS version drop-down list box. All devices that are members of the cluster must be the same device model and run the same ScreenOS version.
4. If you are creating a layer 2 (Transparent mode) cluster, select the Transparent Mode check box.
5. Click OK.

Once you have created the cluster, you can set the cluster ID:

1. In the Device Manager, double-click the cluster in either the FW/VPN Device Tree or the FW/VPN Device List. (Or, either select the cluster and click the Edit icon, or right-click on the cluster and select Edit.
   The Cluster dialog box appears.
2. Select the NSRP option in the Cluster dialog box navigation tree.
   The NSRP configuration screens appear.
3. Set the cluster ID under the General tab. You can also configure any other NSRP link settings in this screen. You can also configure settings in the RTO Mirror and VSD Group Info tabs.
4. Click OK.
Adding Member Devices to the Cluster

To add devices to the cluster:

1. In the Device Manager, right-click the cluster and select New > Cluster Member. The Add Device wizard appears.
2. Enter the name of the device that is being added to the cluster.
3. Follow the directions in the wizard to configure the device.

After you add devices to the same cluster, you need to configure devices in the cluster from within the cluster. Most settings entered on one device in a cluster propagate to the other device.

Note: 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 more information about configurations that do not propagate, 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 for ScreenOS 5.0.0.

To configure a cluster member:

1. In the Device Manager, double-click the cluster in either the FW/VPN Device Tree or the FW/VPN Device List. (Or, either select the cluster and click the Edit icon, or right-click on the cluster and select Edit.) The Cluster dialog box appears.
2. Select the Members option in the Cluster dialog box navigation tree.
3. Double-click the cluster member that you want to configure.
4. Enter the configuration settings you want.
5. Click OK.

Configuring Active/Active Operation

The above directions create a cluster for active/passive operation. That is, all the interfaces on the devices become virtual system interfaces (VSIs) for VSD group 0. To configure the cluster for active/active operation, you need to add a second VSD group. To do this:

1. In the Device Manager, double-click the cluster in either the FW/VPN Device Tree or the FW/VPN Device List. (Or, either select the cluster and click the Edit icon, or right-click on the cluster and select Edit.) The Cluster dialog box appears.
2. Select the Members option in the Cluster dialog box navigation tree.
The Cluster Member screen appears.

3. Right-click in the VSD Definitions area and select New. The Add VSD dialog box appears.
4. Enter a value other than 0.
5. Click OK.

The VSD you added appears in the VSD Definitions list.

**Synchronizing Configurations**

When you add new devices to an NSRP cluster, you must synchronize the configuration and files from one device to another. After synchronizing the configurations and files, you can then synchronize the run-time objects (RTOs).

To synchronize configurations:

1. In the Device Manager, double-click the cluster in either the FW/VPN Device Tree or the FW/VPN Device List. (Or, either select the cluster and click the Edit icon, or right-click on the cluster and select Edit.

   The Cluster dialog box appears.

2. Select NSRP Directives > Flash Sync from the Cluster dialog box navigation tree.

3. Select the device that will be used to synchronize the other device.

4. Click Perform Sync.

The device that has been synchronized is automatically rebooted to activate the new configuration.

**Forcing Master/Backup State**

In an NSRP cluster, one device acts as a master and the other as its backup. When the devices are in an active/passive NSRP configuration, the master handles all firewall and VPN activities while the backup waits to take over when the master steps down.

When the devices are in an active/active NSRP configuration, you create two virtual security devices (VSD) groups. 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; that is, each device is the master of one VSD group and the backup in the other VSD group.

If necessary, for troubleshooting or maintenance, you can force a device to assume a new mode (backup or primary) in a specified VSD group. To do this:

1. In the Device Manager, double-click the cluster in either the FW/VPN Device Tree or the FW/VPN Device List. (Or, either select the cluster and click the Edit icon, or right-click on the cluster and select Edit.

   The Cluster dialog box appears.
2. Select NSRP Directives > Exec Mode from the Cluster dialog box navigation tree.
3. Select the device that will assume a new role.
4. Click Exec Mode. The Mode Selection dialog box appears.
5. Select the mode (backup or primary) that the device is to assume and click OK.
5

Updating Devices

In This Chapter:

- About Updating
- Knowing When to Update
- Using Preview Tools
- Updating Devices
- Tracking Device Updates with Job Manager

After you model or make changes to a device configuration in the Security Manager UI, you must push that device configuration to the physical NetScreen FW/VPN device before those changes can take effect. This chapter details the how to update the running configuration (the configuration on the FW/VPN device) with the modeled configuration (the configuration in the Security Manager UI).

After you have configured your device, you may want to change or update that configuration to have different attributes. This chapter details the process of updating your configuration to reflect a new device configuration and updating that configuration on the device, selected multiple devices, or device groups.

Included are discussions of the basic device updating process, events that occur that require you to update your device, and several integrated tools that enable you to track, verify, and preview the update process. Tools and features introduced include the Update Configuration Directive, Update Notification, Job Manager, and Configuration Summaries.

For devices running ScreenOS 5.0, 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.
### About Updating

Security Manager enables you to group devices with common attributes for updating multiple devices and to track their progress as they undergo updating. Device groups enable you to aggregate devices for convenient updating of groups of devices, providing a distributed approach for evolving your network.

Distributed updating of devices enables you to simplify the process by providing a detailed inventory of appliances and systems throughout your network, across domains, device groups, and device clusters. It also enables you to segment a large number of devices into more manageable common geographic, functional, or logical groups where updates of common devices can occur in isolation of the entire network. This enables efficient network evolution with the least amount of downtime to unaffected devices and areas of your network.

Also, Security Manager enables you to update portions of a device configuration (for example, just modifying a policy), avoiding the more laborious reconfiguration of every aspect of a device, enabling quick updates with less potential for error.

### About Updating Tools

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. Tools that provide this tracking include:

- **Audit Log Viewer.** This tool indicates when a change occurs to any part of the device configuration and which administrator performed the change and when the change was updated on the device. It also provides a history of change details.

- **Report Manager.** This tool collects data from traffic logs on various events that occur over your network and provides a visual representation of them. Reports can be customized 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 tool provides a mechanism to track 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.
About the Update Process

The basic update 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.

   **Note:** While atomic configuration provides fail-safe methods of protecting your ScreenOS 5.0 devices from an undesirable configuration, try to make sure you are satisfied with the configuration you are readying to update to the device.

2. From the menu bar, select Devices > Configuration > Update Config. Security Manager displays the Update Devices dialog box.

3. Select the devices or device groups you want to update and click OK. Security Manager updates the selected devices or device groups with the modeled configuration.

Although the update process is simple, the events that lead to an update process have a number of stages. The following flow table details the events surrounding an example device update.

<table>
<thead>
<tr>
<th>Event</th>
<th>Description</th>
<th>What is Happening</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>You have successfully configured your initial configuration in Security Manager and updated the device and it is running correctly.</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>An event or a trend has occurred on the device that has made the configuration out of date and requires a change. For example, a certain type of attack that the policy of the initial configuration was not set to block has been infiltrating the system. You may not know exactly what has happened yet; you simply can tell the system is functioning differently. The update notification tool may indicate that it detected a change on the DM.</td>
<td></td>
</tr>
</tbody>
</table>
You attempt to find the root cause of the changed behavior by researching information tools like the Realtime Monitor, the Logging tools, the Report Manager, and the Audit Log. After narrowing the types of data you can view in the tools, you determine what type of attack caused the problem. You also determine through the Report Manager what rule was ineffective in blocking the attack.

You add new information to the existing Security Manager configuration, commonly you create a new policy that blocks the recently discovered incoming attacks.

You review the settings you just configured in Security Manager. You preview it with a Configuration Summary and compare it with the current configuration on the device for differences between the two, using the Delta Configuration Summary.

You make the changes you need to correct the configuration so that the device is updated with it.

Using the Update Devices directive, you update the modified configuration on the device. Only the new portion (delta) of the configuration is updated on the device.
Using the Job Information Window in the Job Manager you track the progress of the update real-time, observing the transfer of the configuration from Security Manager to the device go through several states.

If the update attempt is unsuccessful, you record the errors in the Job Information Window and fix them in the portions of the configuration that are creating the problems.

You attempt to update the device again and are successful.

You run a second Delta Configuration Summary to determine if there are any remaining differences between the new configuration and the old configuration on the device.

The Delta Configuration Summary reveals no differences between the new configuration and the old configuration on the device. You have successfully migrated the configuration on the device to accommodate the new requirements of your network.
Knowing When to Update

Many conditions develop that require you to update a current device configuration. Some of them are described here. Generally you need to update a device when you change a configuration, for example, modifying a policy. Note that there are two stages that require tasks associated with the update process:

- Activities involved in determining if you need to update your configuration.
- Activities involved in determining whether you need to update your device with an existing Security Manager configuration.

Security Manager provides tools that enable you to obtain information about changes detected in your firewall environment. A significant change in the environment might mean you need to change a policy. A typical sequence of tasks you might perform to detect changes requiring an update are the following.

- Checking device status
- Checking for error log entries
- Checking administrative changes
- Reviewing reports

Checking Device Status

The most basic condition you want to check is whether the device is active or in a disabled state. This state indicates the Connection State of the device which reports whether the device has an active connection with the Device Server. Security Manager determines the connection status using heartbeat packets to test the connection between the Device Server and the physical device.

To view the connection state of a managed device, use Device Monitor (located under Realtime Monitor). The connection status column displays the current status of the device:

- An Up status indicates the device is connected to the Device Server and is running properly.
- A 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.
- A Never Connection 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.
Knowing When to Update

You may also want to check the configuration status column to determine the state of the configuration. The following figure displays the connection and configuration status in the Realtime Monitor:

<table>
<thead>
<tr>
<th>Device Monitor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Los Angeles</td>
</tr>
<tr>
<td>NewYork</td>
</tr>
<tr>
<td>London</td>
</tr>
<tr>
<td>Paris</td>
</tr>
<tr>
<td>Boston</td>
</tr>
<tr>
<td>Munich</td>
</tr>
<tr>
<td>Tokyo</td>
</tr>
<tr>
<td>Seoul</td>
</tr>
<tr>
<td>Chicago</td>
</tr>
</tbody>
</table>

For more details on using the Device Monitor, see Chapter 10, “Monitoring”.

Checking Error Log Entries

The next task you want to perform is to check the Log Viewer to see if you can detect a common event type that may have caused the device to go down. If you begin to see a pattern of events, you may want to narrow the types of logs forwarded to the Log Viewer to provide a less cluttered, more clear view of the particular type of activity. Log Viewer provides three different ways to restrict the types of logs being forwarded:

- Creating a filter that allows log forwarding based on Log Viewer column criteria
- Enabling log forwarding based on a specific log type
- Creating a severity level that allows only logs with a specified level of importance

You may want to try to track all events that have been sent to the Log Viewer during a recent time period by creating a filter based on column or cell information in the Log Viewer to find only logs that meet the criteria of that particular information. Sample column information that might act as criteria for a filter might be event category, timestamp, and Source Address.

You can launch column and cell filter setting dialog boxes by right-clicking on the column or cell for which you want to set as criteria. Note that when you set filters by cell you can specify a specific value or values greater or equal to or less than or equal to a given value.

For more details on using the Log Viewer, see Chapter 11, “Logging”. For step-by-step instructions on creating a filter, see the Online Help.
Checking for Administrative Changes

Security Manager also provides the Audit Log Viewer that enables you to determine what changes were made to devices on the network that you may not remember or of which you are not aware. Also, a history file that details the administrator who made the change and the date and time of the change is available.

This feature enables you to track what changes were made to your environment. You can track changes by time of logging, administrator name, action, targets, and devices. In addition, you can view details of the change to the object in an object viewer. Also, the Audit Log records a series of action types.

You can select the Audit Log Viewer by clicking on the Audit Log Viewer option in the Navigation Tree. By viewing targets and devices of the Audit Log, you can determine which devices have had a change made to them and which devices need to be updated.

For details on using the Audit Log Viewer, see Chapter 11, “Logging”.

Reviewing Reports

Report Manager is another tool in Security Manager that enables you to identify that you need to modify your configuration. Report Manager can indicate that you are receiving too many attacks of a certain type and order them by an IP address. If you determine that your current configuration cannot block certain attacks, for example scans, you may want to create a new policy that will guard against those attacks and then update the device with the configuration that contains that policy.

You can determine common events by selecting the highlighted event option in the Navigation Tree in Report Manager and then view the incidence of those events in bar graph or pie chart in the Charting Area of Report Manager. Each location within the Charting Area can be expanded to display a finer level of detail. This detail is displayed in the Drill Down section of the Log Viewer. You can then save the detailed versions as separate reports. For example, when viewing the Top Alarms, you can expand a location to view the data that makes up this location.

You may also want to examine specific rules by selecting the Top Rules option in the Navigation Tree and determining how effective the rule is. You may find you need to tune the rule a bit more to block the types of events that may be infiltrating your system.

Note that Report Manager provides three types of reports based on three different criteria: time-based reports, event-based reports, and severity-based reports.

For details on using Report Manager, see Chapter 12, “Reporting”.

USING PREVIEW TOOLS

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. Security Manager supports three types of preview tools:

- **Configuration Summary** which inventories a list of settings in ScreenOS command form you have in your current Security Manager configuration that you want to transfer to the device.

- **Delta Configuration Summary** which compares settings in ScreenOS command form that have been configured for the device in Security Manager that you want to update the device with the commands that already exist on the device. The comparison reveals differences that indicate change you need to make to synchronize the configuration on the device with the new configuration in Security Manager.

- **Running Config** which is the configuration currently on the device.

Both 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.

Note that several phases of the Configuration Summary occur before it either succeeds or fails. View the Output Display region of the Job Information Window to determine the progress of the Configuration Summary. The status field has the following states.

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loading in Progress</td>
<td>Indicates the configuration file is being loaded into the Configuration Summary interpreter.</td>
</tr>
<tr>
<td>In Progress</td>
<td>Indicates the command mapping to the configuration settings is occurring.</td>
</tr>
<tr>
<td>Stopped</td>
<td>Indicates the Configuration Summary process has been halted by an event in the system before it could complete.</td>
</tr>
<tr>
<td>Successful Completion/Failed</td>
<td>Indicates the Configuration Summary process succeeded or failed.</td>
</tr>
</tbody>
</table>

Using a Configuration Summary

When you create a configuration for a device in Security Manager and send the configuration to the device, a series of ScreenOS CLI commands are generated that map to the settings you have created in the GUI. The Configuration Summary displays those commands for you to review.

It is important to make sure you are not transferring a configuration you do not want to send because after the device is updated with the configuration file, it overwrites data that resides in the most recent configuration on the device. For example, if you change a VPN policy in the Security Manager configuration, after you transfer it to the flash memory of the device, you have overwritten the existing VPN policy on your device. So you want to be careful about the information you send and verify that it is what you want.
Running a Configuration Summary

Security Manager provides a way to verify or preview the configuration you are updating on the device called a Configuration Summary. The Configuration Summary is a list of all ScreenOS commands that are equivalent to the parameters you have set in your current Security Manager configuration session that you want to update on the device.

To run a configuration summary:

1. In the Devices menu, click the Configuration option and click Summarize Config. Security Manager displays the Get Configuration Summary dialog box.
2. Click a check box for a device or device group for which you want to run a Configuration Summary and click Ok. Security Manager generates a Configuration Summary in the Job Information window which displays.

For a just-updated device, the Configuration Summary displays the device configuration that matches the configuration currently running on the physical device. If your Configuration Summary process indicate that some of your device parameters are not what you want them to be, you may want to check the following data fields to make sure they have data entered in them or that the data is valid:

- Serial Number
- Device Version
- Username
- Password

You also may want to check the IP address of the device to make sure it is correct. You can also view the status of a Configuration Summary in the Job Manager.

**Note:** You may encounter situations where configuration conversions from Security Manager to ScreenOS do not provide a “one-for-one” mapping between a feature and the command(s) that are equivalent to it. For example, a vsys setting in Security Manager may be equivalent to multiple ScreenOS command lines. Note that device does not have to be reachable or event exist for you to obtain a Configuration Summary. The device database generates the data, not the device.

Also, view the Description field in the Job Information Window to determine the progress of the Configuration Summary. The Description field has the following states.

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Converting Security Manager Data Model to Device Data Model</td>
<td>Indicates the Configuration Summary interpreter is in the process of converting Security Manager GUI objects to ScreenOS CLI commands.</td>
</tr>
<tr>
<td>Success/Failed</td>
<td>Indicates the outcome of the Configuration Summary process, whether it succeeded or failed.</td>
</tr>
</tbody>
</table>
Using a Delta Configuration Summary

A Delta Configuration Summary essentially compares what configuration currently exists on the device and compares it to the configuration with which you are readying to overwrite it. The Delta Configuration Summary then displays the differences between the configuration you see in the Security Manager UI and the configuration on the physical device. The Delta Configuration Summary produces four sets of data:

- The configuration detected on the device but not in Security Manager.
- The configuration detected in Security Manager but not on the device.
- The configuration detected on both the device and Security Manager but has been reordered.
- The configuration that is set to be sent to the device from the Security Manager host on the next update.

You should use the Delta Configuration Summary after you update a device to ensure that the management system imported the physical device configuration as you expected.

**Note:** Delta configuration summaries are helpful tools for ongoing device maintenance, too, particularly for devices that are managed locally both by a device administrator using CLI commands or the WebUI and remotely by a Security Manager administrator using the Security Manager UI. Because the UI device configuration can overwrite the physical device configuration, you should always confirm the commands that are sent to the device.

Conflicts can arise when an administrator configures the device directly using the command-driven ScreenOS environment and another administrator configures parameters for the device in the GUI-driven Security Manager. When the Security Manager administrator then tries to update the GUI configuration on the device, the CLI-created configuration may be overwritten.

Typically, you want to only update the device with data that is distinct from the data on the device (the second bullet). This approach provides a less memory-intensive transfer and provides no risk of unsettling already established data.

For example, you may determine from a Delta Configuration Summary that 90 percent of your device configuration matches the configuration you are going to transfer to the device. The other 10 percent comprises new settings, for example, Shared Vsys settings, a new OSPF virtual routing instance with new areas created for it, and an MD5 authentication setting with a specified key string.

Also, note that the Delta Configuration can be useful in learning of updates in the device that have not been recorded yet on the Security Manager configuration (first bullet). You may not want to overwrite these device-distinct settings.

Note that you may want to run a Delta Configuration Summary two times. Once before you have overwritten the current configuration with your new configuration to identify the new settings you are sending to the device.
You may want to run a second Delta Configuration Summary after you have updated the device with the new configuration to make sure no differences exist between the configuration on the device and the configuration you sent. For a just-imported device, the Delta Configuration Summary should display zero deltas for any of the categories.

A view of a typical Delta Configuration Summary is shown in the following figure.

Running a Delta Configuration Summary

To run a Delta Configuration Summary:

1. In the Devices menu, click the Configuration option and click Summarize Delta Config. Security Manager displays the Get Delta Config Summary dialog box.
2. Click a check box for a device or device group for which you want to run a Delta Configuration Summary and click Ok. Security Manager generates a Delta Configuration Summary in the Job Information window which displays.
UPDATING DEVICES

After you have determined you need to update a device, you now need to perform the update configuration. To update the device with new attributes, you simply invoke an update process using the Update Device Config directive from the Devices Menu.

Note that this process is similar to a first connection and importing of a configuration from the standpoint that you are simply updating data on the device.

To update one or multiple devices, perform the following tasks:

1. Make sure you have completed your new configuration and that you are satisfied with the settings in it.
2. Run a Configuration Summary on the device. View the settings and make sure you want to update the configuration on the device.
3. Run a Delta Configuration Summary and make sure no conflicts exist between the configuration on the device and the configuration in Security Manager that you want to update on the device. If you find conflicts, make adjustments in the configuration that needs to be modified to match the correct configuration.
4. Click the Devices menu and select the Update Device Config option. Security Manager displays the Update Devices dialog box.
5. Click one device, multiple devices, or a device group to select a device or devices for updating.
6. View the Job Manager Information Window to see the states the update undergoes. The first state is Loading and the final state for a successful update is Completion. For more detail on device states, see “Understanding Update Device States” on page 184.
7. View the Job Information Window in the Job Manager at the end of the update. If the update is successful, then Security Manager displays all the commands that have been converted from Security Manager parameters in the Job Manager Information Window. For more information on the Job Information Window, see “About the Job Information Window” on page 182.
8. Run another Delta Configuration Summary to ensure that no conflicts between the running configuration and the modeled configuration exists.

Updating Multiple Devices

One of the powerful features of Security Manager is its ability to update many devices at once, eliminating the time-intensive task of updating devices one by one. After you determine you need to change an existing configuration on a device, you need to perform a configuration update. You can update multiple devices in two ways:

- You can access selected multiple devices that appear in the Device List.
- Creating a device group and selecting it.
Chapter 5 Updating Devices

Updating Device Groups

A device group is a logical collection of devices with similar attributes placed into one object that enables you to locate, configure, and update devices in an efficient way. Useful ways to organize devices into groups is by geography, function, use, size, and types of traffic that passes through the devices (for example, heavy use of graphics, such as a medical imaging environment).

Typically, you first create a group comprising of multiple devices that have common attributes and add appropriate devices to the group. After performing this task, you can update the group as one object with individual devices being modified with the same settings. You create a device group by clicking the FW/VPN Devices option under the Device Manager option in the Navigation Tree. Then click Add (+) and select Group. Security Manager displays the New Group dialog box.

You then provide a name for the device group and begin adding devices to the group by clicking on a device in the Non-Members list and clicking on the Add button to move devices to the Members list. Groups can contain both devices and vsys devices.

About Atomic Configuration

Security Manager provides a fail-safe feature for NetScreen FW/VPN Devices that have been configured in ScreenOS 5.0 that ensures a current valid configuration is not overwritten by a flawed configuration in flash memory. This feature is known as atomic configuration.

The Security Manager atomic configuration feature implies that a configuration update on the device is either executed completely and without errors or is not performed at all, preventing any type or error-prone or flawed configuration to reside on the device. Note that the atomic configuration mode is always on.

Note the following attributes about atomic configuration. The current configuration on the device is saved, locked and timer started. New commands are sent to the device. The configuration cannot be saved until the configuration is unlocked. If all new commands are successfully updated on the device, the configuration is unlocked and saved. If an error occurs, the device is reset, restoring a previous configuration. If an invalid command causes the device to lose communication with Security Manager, the timer expires and the device automatically resets, restoring the previous configuration.

Note: When updating vsys devices, atomic configuration occurs only for the root vsys.
**Tracking Device Updates with Job Manager**

You can track device updates and other tasks using the Job Manager. The Job Manager provides a mechanism to track the status of running and completed jobs and control running jobs in the system. It provides status for a set of directives that are described in the “Managing Devices” chapter. Some of these directives can be issued for a single device or a group of devices.

Note that the Job Manager is not used to initiate these directives, but to view their execution status. You initiate directives from various areas in the Security Manager environment, including the Devices and Tools menus in the Security Manager toolbar.

For details on using the Job Manager, see Chapter 4, “Configuring Devices”.

**Using the Job Manager**

You may find it helpful to view the Job Manager and learn the various types of information it displays pertaining to a configuration update. To access the Job Manager, click the Job Manager option in the Navigation Tree. Security Manager displays the Job Manager Window shown in the following figure:
Review the various areas of the Job Manager to understand the types of activities and information it provides.

<table>
<thead>
<tr>
<th>Area</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Controls</td>
<td>Buttons that enable you to control the view of jobs and job types including Expand All (displays all devices undergoing tasks associated with a directive type) and Collapse All (displays just the directive type).</td>
</tr>
<tr>
<td>Job Type List</td>
<td>Displays the names of job types and associated time stamp completion status information.</td>
</tr>
<tr>
<td>Notification Controls</td>
<td>Enables you to manually view job completion status for either a single job or a job batch.</td>
</tr>
<tr>
<td>Job Information</td>
<td>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.</td>
</tr>
</tbody>
</table>

Note that you see an update job in the Job Type list in the Job Manager dialog box only if Security Manager is running an update job or if you have previously run an update job. Note that all completed update jobs are still in the list. If you are not running an Update Configuration, Job Manager will not display a Update Configuration folder in the Job Type list.

About the Job Information Window

To observe the states a device undergoes during a configuration update, you need to view the Job Information Window. To access the Job Information Window to view device states, perform one of the following:

- To view output on progress of all device configuration updates currently running, simply double-click the Update Device option in the Job Manager Window. You also can launch several update jobs for different devices where each one appears as a separate job in the list.
- To view output on progress of a specific device configuration update job currently running, click the Update Device option in the Job Manager Window to display a list of current devices undergoing an update. Double-click the device for which you want to view output of its update progress.

You can view the stages that a device undergoes in an update process along with associated status, error, and warning messages in real-time in the Job Manager Job Information Window.

You may find it helpful to review the Job Information Window. The Percent Complete Region displays progress status for each job in the job batch. Progress status is shown as a percent value in varying increments in the Percent Complete Region up until the job has completed successfully when the progress status displays 100 percent. The Output Display Region displays all errors, warnings, device verification output, and device state information associated with the job.
An example Job Information window undergoing an update is shown below:

The following table describes the fields and areas in the Job Information Window:

<table>
<thead>
<tr>
<th>Field/Area</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job Type Field</td>
<td>Indicates the type of task being tracked (an update).</td>
</tr>
<tr>
<td>Time Stamp Field</td>
<td>Indicates the time when the update began.</td>
</tr>
<tr>
<td>Job Status Field</td>
<td>Indicates the current state of the update.</td>
</tr>
<tr>
<td>Number of Jobs Completed</td>
<td>If the current job contains multiple devices being updated, displays the devices being updated.</td>
</tr>
<tr>
<td>Percent Complete Region</td>
<td>Indicates the proportion of the entire update that has been successfully performed (as a percent). If multiple devices exist, displays the proportion of the entire update for each device that has been successfully performed (as a percent).</td>
</tr>
<tr>
<td>Device Name Field</td>
<td>Indicates the name of the device that is being updated.</td>
</tr>
<tr>
<td>State Description Field</td>
<td>Indicates the current state of the update. The State Description field provides more detail than the Job Status field.</td>
</tr>
<tr>
<td>Completion Level Field</td>
<td>Indicates the proportion of the entire update that has been successfully performed.</td>
</tr>
<tr>
<td>Output Display Region</td>
<td>Displays content of the update, including commands that have been interpreted from the Security Manager DM into ScreenOS commands, error messages, and existing commands deleted from the device.</td>
</tr>
</tbody>
</table>
Note the two levels of jobs that the Job Manager tracks:

<table>
<thead>
<tr>
<th>Job Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single Job</td>
<td>Includes one entity for which a task is being performed.</td>
</tr>
<tr>
<td>Job Batch</td>
<td>Includes multiple entities associated with the task being performed. For example, on an Update Devices job, there may be multiple devices being updated with new configuration parameters.</td>
</tr>
</tbody>
</table>

The Job Manager either tracks the progress of one discrete entity in the instance of the single job or the progress of each individual job and the progress of the aggregate effort for multiple entities in the job batch.

If there are multiple jobs, the progress status tracks percent complete of all the jobs running. After you are in the Job Manager Information Window, to obtain the job status for the individual device (including error messages and level of completion), simply click the device you want to examine in the Percent Complete box. Security Manager then displays only the output associated with the update of that device in the Output Display Region.

You may want to view all active updates and may want to specify a filtered view of all jobs with errors. If you are updating a single device, you may want to launch the Job Manager Information Window manually and refresh with a less frequent rate as you do not want to view any other jobs. Only the device you are updating may be of interest to you.

**Understanding Update Device States**

After you begin the update process, the device undergoes several states in the same way it does when it has initially imported a configuration. You can view the current state in real-time in the State Description field of the Job Information Window as the update changes from state to state. The following table describes a list of common states that appear in the sequence in which they are displayed in the Description field.

<table>
<thead>
<tr>
<th>Device State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>Indicates no update activity has occurred on the device.</td>
</tr>
<tr>
<td>Loading in Progress</td>
<td>Indicates Security Manager is sending the update image into the Flash memory of the device.</td>
</tr>
<tr>
<td>Pending</td>
<td>Indicates the device has begun to accept 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 Security Manager configuration are being changed to corresponding ScreenOS CLI commands that will reside on the device.</td>
</tr>
<tr>
<td>Completion/Failed</td>
<td>Indicates the device has either successfully been updated with the new configuration (Completion) or has been unable to be updated, generating errors (Failed).</td>
</tr>
</tbody>
</table>
Unlike performing an initial add device session, you do not need to consider whether you are updating a ScreenOS 4.0.x or ScreenOS 5.0 device because each device responds to an update the same way.

**Note:** There are no differences in the way either a ScreenOS 4.0 or ScreenOS 5.0 device responds to a configuration update that has been updated on the device.

### Understanding Errors in the Update Process

You may encounter several different types of errors when you attempt to update the device with modified configuration. A typical error is an instance where the device received configuration settings it did not expect to receive. If the device could not connect to the Device Manager properly, Security Manager displays a message that indicates the Job Status is “Failed.”

If the device connects to the Device Manager, it may still fail. You can tell if it fails when Security Manager displays error codes and error messages in the Job Manager Information Window. Also, check the Connection Status and Configuration Status columns for the device in the Realtime Monitor to determine if the device is running.

Another common error is an instance of the connection between the device server and the device has been lost during the update process. An instance where the device receives an update that it did not expect to receive is shown in the following output.

When an device is updated, Security Manager runs a Delta Configuration Summary to determine whether there is any difference between the configuration that was updated on the device and the configuration version of what Security Manager previously detected on the device. If there is a difference, the output displays indicating the problem.

Note the different stages of the output process shown in the Output Display Region of the Job Information Window when an error occurs.

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Error Message</th>
<th>Inactivated Command</th>
<th>Commands Deleted from Device</th>
<th>New Commands updated on the Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation Type</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Error Code:**
  - **Error Text:** Incorrect command during update device: Configuration tree is not a sub-tree of device.
  - **Error Details:**
    - **Error Indicator:**
      - **Detail of the diff:**
        - `configset@configuration>configset@clear-on-disconnect`: true -> empty
        - `configset@configuration>configset@clear-on-disconnect`: true -> empty

- **New Commands updated on the Device:**
  - `pppoe-name-untrust clear-on-disconnect
  - set policy id 700000 from trust to untrust Any Any permit
  - set policy id 700001 from trust to untrust Any Any permit
  - ping
  - save
  - Configuration command to device ...
  - Device Warning on command:
    - `set policy id 700000 from trust to untrust Any Any permit
    - policy id = 700000
    - Verify configuration ...
    - Verification failed. Configuration tree is not a sub-tree of device tree.
    - **Detail of the diff:**
      - `configset@configuration>configset@clear-on-disconnect`: true -> empty

NetScreen-Security Manager 2004 185
Review this example to follow the flow of events during a failed update. Note the output shows the removal of existing commands on the device, beginning with the output statement:

Generating Removing CLI Commands

Also note the output shows the set of commands that are distinct from the existing configuration on the device, beginning with the output statement:

Generated 5 Delta Config CLI Commands

In this example, note that the configuration could not set the command called:

pppoe name untrust clear-on-disconnect

This error may be caused by another administrator who has disabled the command on the device. The verification process has detected a difference between settings on the device and settings in the Device Manager.
SECTION 3: MANAGING
Managing Devices

In This Chapter:

- Upgrading Firmware on Devices
- Installing and Displaying License Keys
- Activating Subscription Services
- Updating the Attack Database
- Updating AV Pattern Files
- Miscellaneous Device Operations
- Managing Device Capabilities

This chapter describes device management tasks that are not described in other chapters. The Job Manager tracks the status of some of the device management tasks described in this chapter. For more information about Job Manager and the Job Information window, see Chapter 5, “Updating Devices.”
UPGRADING FIRMWARE ON DEVICES

Whenever upgraded ScreenOS firmware is available, you can upload the new image file to one or more NetScreen FW/VPN devices through the Security Manager UI. The firmware upgrade process consists of two basic steps:

1. Use the Firmware Manager to load image files onto the Device Server.
2. Use the Device Manager to select the device(s) and the firmware version to be upgraded on the device(s) from the Device Server.

Note: Security Manager does not support firmware downgrades. That is, you cannot use Security Manager to install an earlier version of ScreenOS firmware than is currently running on the device.

Loading Image Files

To load an image file onto the Device Server:

1. Select Tools > Firmware Manager.
   The Firmware Manager dialog box appears.
2. Click the Add icon to browse to the location of the image file on your PC.
   The Open dialog box appears.
3. Select the image file to be loaded onto the Device Server.

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 NetScreen, for example, ns5xp.4.0.3r2.0.

4. Click Open. The name, version, and applicable devices for the image file appears in the Firmware Manager dialog box.

Note: If you will be upgrading firmware on FW/VPN devices that are currently running ScreenOS 4.x, you need to install a TFTP server on the Security Manager Device Server host. The Device Server uses TFTP to upload the firmware onto ScreenOS 4.x devices. For more information, see the NetScreen-Security Manager 2004 Installer’s Guide.

Upgrading the Firmware on Devices

To upgrade the firmware on one or more devices:

1. Select Firmware > Change Device Firmware from the Devices menu. The Change Device Firmware dialog box appears.
2. Select the device(s) or group of devices on which firmware is to be upgraded.
Upgrading Firmware on Devices

If you select different types of devices, make sure that you have loaded the same 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 type of device must exist on the Device Server and must be the same ScreenOS version.

3. Select the firmware version to be installed on the devices.
4. Click Next.

The Firmware Update Availability dialog box appears, showing the selected device(s) and firmware to be installed.

**Note:** The Automate ADM Transformation option allows the Abstract Data Model (ADM) for the device to automatically update when the firmware is uploaded. If you deselect this option, the firmware is uploaded onto the device, but you will not be able to manage the device from the UI until the ADM for the device is updated. For example, you can deselect this option to first verify that the device is properly operating with the uploaded firmware before allowing it to be managed from the Security Manager UI. You will later need to reconcile the firmware that you uploaded on the device with the ADM, as described in “Adjusting the Firmware Version” on page 191. For more information about the ADM and Security Manager components, see “Managing Device Capabilities” on page 200.

5. Click Finish.

The Job Information window displays the status of the upload. The device automatically reboots after the firmware is installed.

### Adjusting the Firmware Version

During the import or update of devices, you are alerted if Security Manager detects a mismatch between the firmware that is actually running on the device and what is shown in the Security Manager UI via the ADM. This can occur when the firmware on a device is changed by a local administrator through the WebUI or through a console, Telnet, or SSH session. This can also occur if you selected the Automate ADM Transformation option in the Firmware Update Availability dialog box while performing a firmware upgrade in the Security Manager UI. (See “Upgrading the Firmware on Devices” on page 190.)

To reconcile the firmware version:

1. Right-click a device from the FW/VPN Device Tree or the FW/VPN Device List tab in the Device Manager and select Adjust OS Version. The Adjust OS Version Wizard appears.
2. Follow the directions in the wizard.
**INSTALLING AND DISPLAYING LICENSE KEYS**

Some NetScreen FW/VPN devices support the activation of optional features or the increased capacity of existing features through the installation of license keys.

**Installing License Keys**

The procedure for obtaining a license key is as follows:

1. Contact the value-added reseller (VAR) who sold you the NetScreen FW/VPN device, or contact NetScreen 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:

1. Right-click a device from the FW/VPN Device Tree or the FW/VPN Device List tab in the Device Manager 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.

**Displaying License Key Information**

To see which license keys are installed on a device, and the features and capacities available on the device:

1. Right-click a device from the FW/VPN Device Tree or the FW/VPN Device List tab in the Device Manager and select Admin > Get License Key Info.
2. Click Yes at the confirmation dialog box.
   The Job Information window displays the license key information.
Activating Subscription Services

Certain ScreenOS services, such as internal antivirus or Deep Inspection Signature Service, must be activated 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.netscreen.com/cso. After you have registered your product, you can retrieve the service subscription as described in the following section.

Retrieving a Service Subscription

To obtain the subscription for a service:

1. Select Entitlement > Get Entitlement from Entitlement server from the Device menu.
   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.
Deep Inspection is a mechanism for filtering the traffic permitted by the NetScreen FW/VPN device. Deep Inspection uses an attack object database which contains all the predefined attack objects, organized into attack object groups by protocol and severity level. To use the predefined attack objects, you must download the database from a server at https://services.netscreen.com/restricted/sigupdates.

**Note:** You must first obtain a subscription for your NetScreen FW/VPN device in order for the device to gain access to the attack object database server. For more information, see “Retrieving a Service Subscription” on page 193.

### Updating the Database Immediately

You can update the attack object database on the NetScreen FW/VPN device immediately with the database stored on the attack object database server. For this operation to work, you must first configure the attack object database server settings (see Chapter 4, “Configuring Devices”).

To update the attack object database on a device:

1. Select Deep Inspection > Update Attack Database from the Devices menu. The Update Attack Database 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.

### Checking the Attack Database Version

You can check if the attack object database on the server is more recent than the one on the NetScreen FW/VPN device. This can help you determine if you need to update the database immediately.

To 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 check.
Updating AV Pattern Files

Some NetScreen FW/VPN 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.

Updating the AV Pattern File

To update the AV pattern file for a device:

1. Select AV Scan Manager > Update Pattern from the Devices menu.
   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.
MISCELLANEOUS DEVICE OPERATIONS

This section describes other device management tasks that you can perform via the Security Manager UI.

Restarting Devices

You can restart one or more selected devices, or a group of devices. To restart one or more devices:

1. Select Reboot Device from the Devices menu. 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 NetScreen FW/VPN 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 (see Chapter 4, "Configuring Devices").

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 NetScreen FW/VPN 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 Chapter 4, "Configuring Devices"), 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. Select NTP > Perform NTP Time Update from the Devices menu. 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 NetScreen FW/VPN devices ship with the same default login and password for the root administrator. Therefore, you should change the login and password for the root administrator as soon as possible and as often as necessary. There can be only one root administrator per FW/VPN device. The root administrator has the following privileges:

- Manages the root system of the NetScreen FW/VPN 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
- Resets the device to its default settings
- Updates the firmware
- Loads configuration files

Once 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 FW/VPN device:

1. Right-click a device from the FW/VPN Device Tree or FW/VPN Device List tab in the Device Manager and 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.
Failing Over/Reverting Back Interfaces

Some NetScreen FW/VPN 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 FW/VPN device to fail over to the backup interface:

1. Right-click a device from the FW/VPN Device Tree or the FW/VPN 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 FW/VPN device to revert back to the primary interface:

1. Right-click a device from the FW/VPN Device Tree or the FW/VPN 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 ever 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 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 FW/VPN Device Tree or FW/VPN 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 Chapter 3, "Adding Devices".

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.
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. Right-click a device from the FW/VPN Device Tree or FW/VPN Device List tab in the Device Manager 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

**Note:** This task is only applicable to added FW/VPN devices running ScreenOS 4.x with dynamic IP addresses.

To display the CLI configuration commands for a device, right-click a device from the FW/VPN Device Tree or FW/VPN Device List tab in the Device Manager and select Admin > Show Device Commands.

Finding Usages

To locate groups, vsys, policies, and VPNs in which a specific device is referenced, right-click a device from the FW/VPN Device Tree or FW/VPN Device List tab in the Device Manager and select Find Usages. The Find References box appears.
MANAGING DEVICE CAPABILITIES

This section presents a detailed description of how Security Manager components allow you to add, configure, update, and manage NetScreen FW/VPN 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 NetScreen FW/VPN devices that are running different ScreenOS versions. For example, a NetScreen-5XT may run ScreenOS 5.0.0, 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 Security Manager and also make upgrading the software on your NetScreen FW/VPN 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, etc.) 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, VPN policies, etc. 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.
Device 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.
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.
Objects represent reusable information, such as network addresses, individual users and user groups, and commonly used configuration data. In Security Manager, objects are shared objects, meaning they are shared between the global domain and all subdomains.

Objects are the building blocks of the 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 policy rule.
About Objects

Objects created in the global domain are available in all subdomains, but objects created in a subdomain are only available in that subdomain.

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.

Object Types

The Security Manager UI groups most objects under Object Manager, and the VPN-related objects under VPN Manager.

Use Object Manager to view, add, edit, and delete the following objects:

- **Network and Address Translation:**
  - 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:**
  - Attack Objects represent signature patterns and service contexts for known attacks.
  - AV Objects define the server that contains your virus definitions and AntiVirus software.

- **Users and Authentication:**
  - User Objects represent RAS users on your network.
  - Authentication Servers represent the servers in your network used to authenticate 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.

Use VPN Manager to view, add, edit, and delete the following objects:

• **Protected Resources** represent the network component, a network service, and the NetScreen FW/VPN device that protects that component and service.

• **IKE Phase 1 Proposals** represent the phase 1 proposals used to establish a secure and authenticated communication channel between two VPN members.

• **IKE Phase 2 Proposals** represent the Security Associations for services (such as IPsec) that require key material and/or parameters, as exchanged by two VPN members.

### Imported Objects

If you already have objects defined in your existing Global Pro management system or on the device itself, you can import those objects into Security Manager. When importing device configurations and their domains from Global Pro, Security Manager also imports all objects that are defined for those domains. During this import process, Security Manager determines if the object is accessible by a single domain or accessible by all domains.

When importing device configurations directly from the managed device, Security Manager imports the following objects:

<table>
<thead>
<tr>
<th>ScreenOS Firewall</th>
<th>... Become this NetScreen-Security Manager Object</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address Book Objects</td>
<td>Address Objects represent components of your network (hosts, networks, servers, etc.)</td>
</tr>
<tr>
<td>VPN Objects</td>
<td>VPN Objects represent IKE Phase 1 and Phase 2 proposal lists.</td>
</tr>
<tr>
<td>Protected Resources</td>
<td>Protected Resources represent services on a specific network component. You can use Protected Resource objects to create VPNs.</td>
</tr>
<tr>
<td>User Objects</td>
<td>User Objects represent users that access a protected network. You can use user objects to define create remote access solutions using VPN tunnels and ANG.</td>
</tr>
<tr>
<td>Schedule Objects</td>
<td>Schedule Objects represent specific dates and times. You can use schedule objects for device configuration or policy deployments, software upgrades, and report generation.</td>
</tr>
<tr>
<td>Service Objects</td>
<td>Service Objects represent services running on your network, such as FTP, HTTP, and Telnet. 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 run on your network.</td>
</tr>
</tbody>
</table>
Chapter 7 Configuring Objects

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 Security Manager to specify the network components you want to protect:

- **Firewall Policies.** Use address objects or groups to specify the source and/or destination of network 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.netscreen.com) of the address object
  - **Netmask.** Netmask of the address object
  - **Comment.** A description of the address object

When you initially deploy the 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 the address objects, they appear in the both 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.

The following sections detail each Address Object type.
Adding a Host Address Object

To add a host address object:

1. In the Navigation Tree, open the Object Manager and select Address Objects. The address object tree appears.
2. In the main display area, click the add icon and select Host.
3. Enter a name for the address object.
4. Select a color to represent the address object.
5. Enter a Comment about the host.
6. 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.
7. 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.
2. In the main display area, click the add icon and select Network.
3. Enter a name for the address object.
4. Enter the IP address and netmask of the network.
5. Select a color to represent the address object.
6. Enter a Comment about the network.
7. 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 firewall 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.
2. In the main display area, click the add icon and select Group.
3. Enter a name for the group.

**Note:** Address Object group names must be unique; you cannot name an address object group the same name as an existing address object.

4. Select a color to represent the group.
5. Enter a Comment about the group.
6. 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.
7. Click Add. The selected address objects now appear in the member list.
8. 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.
Configuring Schedule Objects

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)
  - After Hours Schedule (6:01 PM to 7:59 AM on Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday)
  - Weekend Schedule (8:00 AM to 6:00 PM on Saturday, Sunday)
- Combine a one-time and recurrent schedule to define a repeated time interval.

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).
Chapter 7 Configuring Objects

CONFIGURING ATTACK OBJECTS

Attack objects contain attack patterns for known attacks that attackers can use to compromise your network. Attack objects don't work on their own—they need to be part of a rule before they can start detecting known attacks and preventing malicious traffic from entering your network.

To use attack objects in your firewall rules, enable Deep Inspection in the Rule Option column of a firewall policy. Deep Inspection is supported by the NS-5GT, the NS-HSC, and all devices running ScreenOS 5.0.

You can view, edit, and create attack objects. You might want to view an attack object to find out more about the attack it detects and the signature it uses. Or, you might want to edit the context of an attack object that is producing too many false positives on your network. Maybe you heard about some new virus or Trojan that is sweeping the Internet and you want to create a custom signature to detect it as it enters your network.

Attack Object Types

Security Manager supports two types of attack objects:

- Signature Attack Objects
- Protocol Anomaly Attack Objects

The following sections detail each attack object type.

Signature Attack Objects

Attack objects detect known attacks using attack signatures. An attack signature is a pattern that always exists within an attack; if the attack is present, so is the attack signature. Security Manager uses stateful signatures to detect attacks. A stateful signature is a signature that not only knows the pattern it is attempting to find, but also knows where to look for that pattern. Stateful signatures produce very few false positives because they understand the context of the attack and can eliminate huge sections of network traffic they know the attack won’t be in.

Stateful signatures are much smarter than regular signatures: they know the protocol or service used to perpetrate the attack, they know the direction and flow of the attack, and they know the context in which the attack occurs. Obviously, though, a signature can’t contain all this information within the attack signature pattern—the data must be associated with the signature, but not actually part of the pattern itself. NetScreen does this by combining the attack pattern with service, context, and other information into a neat little package called an attack object.

Protocol Anomaly Attack Objects

Signature attack objects can only detect known attacks, because a pattern needs to be created before it can be matched. Thus, signature attack objects do not detect new attacks or attacks that resist characterization. However, Security Manager features Protocol Anomaly Detection using protocol anomaly attack objects to find unknown or
sophisticated attacks that violate protocol specifications. Protocol Anomaly Detection works by comparing traffic to what is not considered harmful from a protocol perspective. Security policy rules with protocol anomaly attack objects match on traffic that does not conform with RFCs and common RFC extensions.

**Predefined & Custom Attack Objects**

Security Manager includes predefined attack object groups that you can use in firewall policies to match traffic against known attacks. You can also create custom attack objects and attack object groups to detect attacks specific to your network.

**Viewing Predefined Attack Objects**

In Object Manager, click Predefined Attack Objects to display the list of predefined attack objects that represent known and unknown attack patterns. The Attack Object Tree tab (default view) is useful for viewing the membership of attack groups. To display all members of an attack group, double-click the group.

The Attack Object Table tab is useful for viewing details about an attack object. The Attack Table tab displays all attacks in a table format and includes the following information:

- Name of the attack object
- Type of attack object: signature, anomaly, or group
- Attack severity (Major, Minor).
- Miscellaneous comment about the attack object

You cannot create, edit, or delete predefined attack objects, but you can update the list of attack objects using the Attack Update Client, detailed below.

**Updating Predefined Attack Objects**

To keep your Attack Object database up-to-date, download new Attack Objects weekly from NetScreen using the Attack Update Client. Updates can include:

- New descriptions or severities for existing attack objects
- New attack objects
- Deletion of obsolete Attack Objects

From the menu bar, click Tools > Update Attacks to display the Attack Update Client, then follow the wizard to update your list of predefined attack objects. For step-by-step instructions on using the wizard, see the Online Help topic “Updating Attack Objects”.
Creating Custom Attack Objects

You can create custom attack objects to detect new attack or customize an existing attack to meet the unique needs of your network.

**Note:** You cannot create new protocol anomaly attack objects.

To add an attack object:

1. In the navigation tree, double-click Object Manager and select Attack Object > Custom Attack Objects. In the main display area, click the Signatures tab.
2. Click the Add icon. The New Attack dialog box appears.
3. Enter a name for the attack (the name must begin with CS:). You might want to include the protocol the attack uses in the attack name.
4. Select a severity for this attack: info, warning, minor, major, critical.
5. Select a color and enter a comment for the attack, if desired.
6. In the Pattern table, click the Add icon to configure a pattern for the attack object. In the Pattern Name dialog box, enter:
   - In the **Pattern Name** box, enter a name for the pattern you want this attack to match.
   - In the **Pattern** box, enter the regular expression you want to match. Security Manager supports the following expressions:

<table>
<thead>
<tr>
<th>Regular Expression</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>\0&lt;octal-number&gt;</td>
<td>For a direct binary match</td>
</tr>
<tr>
<td>\X&lt;hexadecimal-number&gt;\X</td>
<td>For a direct binary match</td>
</tr>
<tr>
<td>[&lt;character-set&gt;]</td>
<td>For case insensitive matches</td>
</tr>
<tr>
<td>.</td>
<td>To match any symbol</td>
</tr>
<tr>
<td>*</td>
<td>To match 0 or more symbols</td>
</tr>
<tr>
<td>+</td>
<td>To match 1 or more symbols</td>
</tr>
<tr>
<td>?</td>
<td>To match 0 or 1 symbols</td>
</tr>
<tr>
<td>()</td>
<td>Grouping of expressions</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>[&lt;start&gt;-&lt;end&gt;]</td>
<td>Character range</td>
</tr>
<tr>
<td>[^&lt;start&gt;-&lt;end&gt;]</td>
<td>Negation of range</td>
</tr>
</tbody>
</table>

- Select a context for the attack. The context defines the exact location in the packet you want the NetScreen FW/VPN to search for the attack pattern. Selecting a context enables you to make precise matches, reducing false positives and improving performance.
Configuring Attack Objects

Security Manager supports the following contexts:

<table>
<thead>
<tr>
<th>Context</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP Command</td>
<td>Matches the attack pattern against an FTP command.</td>
</tr>
<tr>
<td>FTP Username</td>
<td>Matches the attack pattern against the FTP user name (RFC 959, #4.1.1).</td>
</tr>
</tbody>
</table>
| HTTP URLParsed   | Matches the attack pattern against the URL after it has been normalized and parsed. All parameters of the URI are skipped (anything after the '?' is skipped). The NetScreen FW/VPN device performs the following normalizations on the URL:  
  • % (hexadecimal) decoding  
  • %u decoding  
  • unicode normalization  
  • normalize directory traversals ('..' and './')  
  • remove double slashes - '/\'
  • convert tabs to space  
  • convert DOS '\\' to '/'
  • remove NULL characters '%00'
| SMTP From        | Matches the attack pattern against the SMTP 'MAIL FROM' command line.       |
| SMTP Header From | Matches the attack pattern against the SMTP 'From:' header.                 |
| SMTP RCPT        | Matches the attack pattern against the SMTP 'RCPT TO' command line.         |
| SMTP Header To   | Matches the attack pattern against the SMTP 'To:' header.                   |
| Stream           | Matches the attack pattern against the entire stream of data.               |

7. Click OK to save the pattern, then click OK again to save the attack object.

Creating Attack Groups

You can create attack groups of custom attack objects to use in your firewall policies. To add an Attack Object group:

1. In the navigation tree, double-click Object Manager and select Custom Attack Objects. In the Attack Object Group tab, click the Add icon to display the new Attack Group dialog box.
2. Enter a name, color, and comment for the attack group.
   
   **Note:** Attack group names cannot be the same as attack object names.

3. Select the custom attack objects or attack groups you want to add to the group by clicking them in the Non-members area (Hold CTRL to select multiple objects); then click Add. To add all objects to the group, click Add All.
4. Click OK to save the group.
**CONFIGURING ANTIVIRUS OBJECTS**

AV objects define the server that contains your virus definitions and AntiVirus software. To create an AV object, select AV Objects and click the Add icon. Enter a name for the object, then configure the AV server parameters:

- **Server Name.** Enter the name of the AV server.
- **Server Port.** Enter the port number on the AV server.
- **Color.** Select a color to represent the object in the Security Manager UI.
- **Comment.** Enter a comment, if desired.
- **Contents.** Configure the protocol that the AV server scans for viruses:
  - **HTTP.** To scan HTTP traffic for viruses, enable HTTP and configure the number of seconds.
  - **SMTP.** To scan SMTP traffic for viruses, enable SMTP and configure the number of seconds.
**Configuring Service Objects**

Service objects represent the IP traffic types for existing protocol standards. NetScreen FW/VPN devices monitor and manage network traffic using these protocols. 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 firewall 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 policy, 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 NetScreen FW/VPN detects packets that use the specified service type.

**Viewing Predefined Services**

A predefined service object represents a standard communication protocol, such as FTP or HTTP. To view predefined service objects, double-click Service Objects in the navigation tree and select predefined Services. The available services appear in the main display area within the Service tree tab, which displays the service objects in a tree format. Select a service group to display the members of that group.

To view service objects in a tabular format, select the Service Table tab. The available services appear in a table that uses the following format:

<table>
<thead>
<tr>
<th>Name</th>
<th>Name of the service object</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Type of the service object: service or group</td>
</tr>
<tr>
<td>Timeout</td>
<td>Service timeout—inactivity timeout after which a session on a NetScreen FW/VPN device is removed</td>
</tr>
<tr>
<td>Category</td>
<td>Classification broadly based on the purpose the service is designed for: email—used for sending and receiving email (POP3, for example) info seeking—used to retrieve specific information from a server (DNS, for example) remote—used for accessing remote servers (telnet, for example) security—allows the access of a remote server securely using well known security mechanisms (HTTPS for example) other—all other services</td>
</tr>
</tbody>
</table>

You can view details for a predefined service object, but you cannot edit that service object. To view in read-only mode, double-click the service object to open it.
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.

To add a service object, in the Object Manager, select Service Objects > Custom Service Objects. In the main display area, click the Add icon to display the New Service dialog box. Select Service, enter a name for the service, then configure the following parameters:

- **Category.** Select a category for the service:
  - Other. All other services
  - Remote. Services used for accessing remote servers (telnet, etc.)
  - Info seeking. Services used to retrieve specific information from a server (DNS, etc.)
  - Security. Services that allow the access of a remote server securely using well known security mechanisms (HTTPS, etc.).
  - Email. Services used for sending and receiving email (POP3, etc.)
- **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 40 minutes.
- **Color.** Select a color to represent this service object in the Security Manager UI.
- **Comment.** Add a comment, if desired.
- **Add the service:**
  - For ICMP services, select the ICMP type and code. For details on ICMP type, see the NetScreen Security Manager Online Help.
  - For other services, select the protocol type and configure the source and destination ports. For multiple ports, add two service entries with different ports.

Service Object Groups

You can group services together as a service object group, then use that group in firewall 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, double-click Object Manager and select 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.

**Note:** Service object group names cannot be the same as service object names.

4. Select the service objects or service object groups you want to add to the group by clicking them in the Non-members area (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: Custom Service & Group**

In this example, you'll 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 Service Objects, select Custom Service Objects. In the main display area, click the Add icon and select **Service**.

2. Configure the object as shown below:

   ![Service Entry](image)

   - **Protocol ID**: TCP
   - **Source Port**: Any, Specific, Range
   - **Destination Port**: Any, Specific, Range
   - **Specific Port**: 113

   Click the Add icon to configure the Ident protocol and ports.

3. Click OK to save the object and return to Custom Service Objects.
Next, create a Remote Mail service group:

1. In Service Objects, select Custom Service Objects. In the main display area, click the Add icon and select Group.
2. Configure the group as shown below:

![Service Group window]

![Non-members]

![Members]

3. Click OK to save the group and return to Custom Service Objects.
Configuring User Objects

User objects represent the users of your managed devices. You can include user objects or groups in firewall policies or VPNs to permit or deny access to individuals or groups. Security Manager supports two types of user objects:

- **Local Users** are users with accounts that are managed by your NetScreen FW/VPN devices. You can create local user groups that include multiple users to simplify user administration and make firewall policies and VPNs easier to create.

- **External Users** and **External User Groups** are 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 226).

Configuring Local Users

Local User Objects represent the user account on your NetScreen FW/VPN devices. To add a local user object:

1. In the navigation tree, double-click the Object Manager, select User Objects, then select Local Users.
2. In the main display area, click the Add icon and select New > User to display the New Local User dialog box.
3. Enter a name, color, and comment for the local group.
4. Select the Enable checkbox 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 NetScreen FW/VPN 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.
5. Click OK.
Configuring Local User Groups

You can organize local users in groups to add multiple users at one time to a firewall policy, and to manage the members without changing the policy. To add a local user group object:

1. In the navigation tree, double-click the Object Manager, select User Objects, then select Local Users.
2. In the main display area, click the Add icon and select New > Group to display the New Local User Group dialog box.
3. Enter a name, color, and comment for the local user group.
4. 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.
5. 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 Security Manager, such as an external RADIUS or SecureID server. When an external user is included in a firewall policy (under Authentication rule options), the NetScreen FW/VPN 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.
2. In the main display area, click the Add icon and select New to display the New External User dialog box.
3. Enter a name, color, and comment for the external user.
4. Click OK to save the external user object.

Configuring External User Groups

External User Group objects represent user groups that are not managed on devices that are not managed by Security Manager, such as an external RADIUS or SecureID server. When an external user group is included in a firewall policy (under Authentication rule options), the NetScreen FW/VPN device uses the external server to authenticate those users.
To add an external user group object:

1. In the navigation tree, double-click the Object Manager, select User Objects, then select External User Groups.
2. In the main display area, click the Add icon and select New to display the New External Group dialog box.
3. Enter a name for the external user group. The name must match the name of the user group as configured on the external server.
4. Enter a color and comment for the external user group.
5. 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 NetScreen FW/VPN device's local database.
   - L2TP: Enables authentication in the L2TP tunnel that users in the group use to connect to the device.
6. Click OK.
CONFIGURING AUTHENTICATION SERVERS

An authentication server provides authentication for Security Manager administrators and remote access services (RAS) users on your network. You can use authentication servers to:

- Set a default authentication server for the global domain and each subdomain.
- Access an external RADIUS or SecureID server to provide authentication.

Configuring Authentication Servers

Select Authentication Servers and click the Add icon. Enter a name, color, and comment for the authentication server, then configure the following parameters:

- **Main Server.** Enter the IP address of the main authentication server.
- **Primary Backup Server.** Enter the IP address of the primary backup server.
- **Secondary Backup Server.** For RADIUS servers only, you can enter the IP address of the secondary backup server (this option is not supported for SecureID servers).
- **Authentication Timeout.** Enter the number of minutes before the authentication check times out.
- **Users.** Enable the server to provide authentication for:
  - Admin Users.
  - Firewall Auth Users.
  - XAuth Users.
  - L2TP Users.
- **Server Type.** Select the authentication server type (RADIUS or SecureID) and configure the necessary parameters.
CONFIGURING IP POOLS

An IP pool is a range of IP addresses within the same subnet. Security Manager uses IP Pool objects to assign IP addresses to RAS users in L2TP VPNs.

An IP Pool object has the following fields:

- **IP Pool Name**: The name of the IP Pool.
- **Start IP**: The beginning of the range of IP addresses included in this 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 this pool, inclusive. The End IP must always be higher than the Start IP.

You use IP Pools when configuring an L2TP VPN. The IP pools you select determine the range of IP Addresses the VPN can use.

Configuring IP Pools

To add an IP pool:

1. In the Navigation Tree, select Object Manager > IP Pools.
2. In the main display area, click the Add icon.
3. Enter a name, color, and comment about the IP Pool.
4. Enter the Start IP and End IP. Enter a range wide enough to accommodate the number of RAS users in your VPN.
5. Click OK to save the IP Pool object and return to Object Manager.
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 allows 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 firewall policy, as detailed below:

**User Objects**

- **OR** If the firewall policy defines authentication for “a” or “b” user objects, the NetScreen FW/VPN device authenticates the user if it is either “a” or “b”.

- **AND** 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 “a” and user “b”). If the firewall policy defines authentication for “a” AND a member of group “b”, the NetScreen FW/VPN device authenticates the user only if those two conditions are met.

- **NOT** If the firewall policy defines authentication for any user object that is not the “c” user (NOT “c”), the NetScreen FW/VPN device authenticates all users except the “c” user.

**User groups**

- **OR** If the firewall policy defines authentication for user group “a” or user group “b”, the NetScreen FW/VPN device authenticates the user if it belongs to either “a” or “b” user group.

- **AND** If the firewall policy defines authentication for user group “a” AND user group “b”, the NetScreen FW/VPN device authenticates the user only if it belongs to both user groups.

- **NOT** If the firewall policy defines authentication for any user group that is not group “c” (NOT “c”), the NetScreen FW/VPN device authenticates all users except those that belong to the “c” user group.

**Group expressions**

- **OR** If the firewall policy defines authentication for user objects that match the description of group expression “a” OR group expression “b”, the NetScreen FW/VPN device authenticates the user if either group expression references that user.
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 Chapter 8, “Configuring Firewall Policies”.

Example: Group Expressions

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 firewall policy that provides access to your protected networks.
Chapter 7 Configuring Objects

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:

   ![External User Groups](image)

   - **Marketing Group**: AI Marketing
   - **Sales Group**: AI sales

2. Next, create a group expression object that references both the Sales and Marketing group, as shown below:

   ![Group Expression](image)

   - **Sales & Marketing**
   - **Comment**: SE and Marcom access
   - **Operands**: Sales Group, Marketing Group

3. Finally, add the group expression object to your firewall rule in the Authentication rule option, as shown below:

   ![Configure Options](image)

   - **Select Authentication** as the Authentication option
   - **Select the authentication server object that represents the RADIUS server used to authenticate your external user groups.**
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.

NetScreen FW/VPN 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.netscreen.com) in addition to using a routable 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).

Configuring Remote Settings

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 (a global DIP represents multiple device-specific DIPs, etc.). 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 configuration:

- **Device**: Select the NetScreen FW/VPN 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.

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 configuration:

- **Device**: Select the NetScreen FW/VPN 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.
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 NetScreen FW/VPN 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.
Chapter 7 Configuring Objects

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). 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 5.0 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:

- An independent CA server is 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.
- An internal CA server is 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 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 Chapter 4, “Configuring Devices”.

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. 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.
  - OSCP. 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 NetScreen FW/VPN 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 FW/VPN 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 CERTIFICATE REVOCATION LISTS

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 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. 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 is the combination of a network component, a network service, a traffic direction, and the NetScreen FW/VPN device that protects that component and service. 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 that can communicate over a network, such as FTP and HTTP. 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 typically outgoing, or outbound from the protected network.
  - Server connections are typically incoming, or inbound to the protected network.
  - To protect incoming and outgoing traffic, select Both.

- **NetScreen FW/VPN device.** The device is the FW/VPN device through which the VPN must connect to reach the protected resource. If the resource can be reached through more than one device, you can add multiple devices to the resource. When you add a protected resource to a VPN, the devices listed 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 can also 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, open VPN Manager and click Protected Resources.
2. In the main display area, click the Add icon to display the Protected Resource dialog box.
3. Enter a name for the protected resource.
4. Select the services you want to permit to this resource, such as FTP, HTTP, NFS, etc. Select Any to permit all services.
5. Select the initiator of the permitted service: Server, a Client, or Both.
6. Select the address object or address group for the resource.
7. Add the FW/VPN 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 FW/VPN device or device group
   c. Select the security zone on the FW/VPN 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, Security Manager automatically generates new configuration and propagates your changes to all affected FW/VPN devices.
- If you change the FW/VPN device that protects a resource, Security Manager removes the previous FW/VPN device from all affected VPNs and adds the new FW/VPN device. However, Security Manager does not configure the VPN topology for the new FW/VPN—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, 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-NetScreen FW/VPN 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.
Configuring IKE Proposals

- **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-NetScreen FW/VPN 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.

Click OK to add the custom IKE object to the management system.
8

Configuring Firewall Policies

In This Chapter:

- About Firewall Policies
- Configuring Firewall Rules
- Validating Firewall Policies
- Installing & Updating Firewall Policies
- Managing Rules & 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. A firewall policy defines access to your network, including allowed services, users, and time periods. You can also use firewall policies to control the shape of your network traffic as it passes through the firewall, or log specific network events.

Using Security Manager features like device groups, zone exceptions, and application-level detection, you can make your firewall policies easier to manage and more efficient.
About Firewall Policies

By default, all NetScreen FW/VPN devices deny all traffic. You create firewall policies 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 NetScreen firewall as a device in Security Manager, you can create a firewall policy, assign it to the device, and install it on that device.

To create a firewall policy, build firewall rules that 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. You can build multiple firewall rules for a single device; these rules combine to create a firewall policy that determines how your NetScreen FW/VPN device handles traffic.

Note: On NetScreen vsys devices, rules defined in the root system do not affect rules defined in virtual systems.

About Rules

A rule is a statement that defines a specific type of network traffic. When traffic passes through the FW/VPN 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. You can create firewall rules, VPN rules, and VPN links, as described in the following sections.

Adding Firewall Rules

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 NetScreen FW/VPN 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 NetScreen FW/VPN device performs when it receives traffic that matches the direction, source, destination, and service.
- **Install On.** The NetScreen FW/VPN device on which the firewall rule is installed. You can install the same rule on multiple devices.

A firewall rule defines a specific list of requirements that the network traffic must meet before it is permitted to pass through the NetScreen FW/VPN device. Network traffic that matches this list of requirements is considered to “match” the firewall rule, and the firewall performs the action specified in the rule. If any requirement is not met, the network traffic does not match, and is denied.
You create firewall rules using the Policy Manager in the UI. If you have multiple firewall rules, you determine the order that rules are applied to network traffic by placing them in the desired sequential order. For details on re-ordering your firewall rules, see "Using Cut, Copy, & Paste" on page 259.

You can also disable a rule in a policy, and negate the source or destination addresses (5.0 devices only).

### Adding VPN Links & Rules

The rules for your rule-based VPNs also appear in the firewall policy.

- **Use VPN Links** for VPNs created in VPN Manager. By default, VPN Manager autogenerated rules are placed at the top of the firewall policy and are executed first. (Because VPN Manager autogenerates the access rules for the VPN, you do not need to manually create them in the policy itself.) To specify the exact location of the autogenerated rules in your policy, you can add a VPN link anywhere in firewall policy.

- **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 firewall policy.

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 policies to control the flow of traffic in a routing-based VPN tunnel.

For details on adding VPN links or VPN rules, see Chapter 9, "Configuring VPNs".

### About Rulebases

A rulebase is a set of rules. Security Manager supports two firewall rulebases:

- **The zone-specific** 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 for 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 two firewall rulebases combine to create the firewall policy. NetScreen FW/VPN devices process and execute rules in the zone-specific rulebase first, then rules in the global rulebase.
Chapter 8 Configuring Firewall Policies

About Firewall Policies

A firewall policy is the combination of both firewall rulebases and all firewall rules into a comprehensive plan that defines how the firewall works on your network. When creating a firewall policy, consider the type, location, and functionality of each NetScreen FW/VPN device in your network.

Typically, a single policy for multiple devices works well for devices that perform similar functions, such as perimeter firewalls. However, you might want to create a separate policy per device when the management system contains separate administrators with regional responsibilities, or when you need to troubleshoot a device issue (use one policy per device to enable an admin to troubleshoot on one device without making policy changes on other devices.

To simplify policy creation, use device groups to build access rules that apply to all your perimeter NetScreen FW/VPN devices, then apply the entire policy to the perimeter device group.

Merging Imported Policies

New devices do not have existing or default policies. However, when you import a device configuration, Security Manager automatically imports all existing policies for the device. To simplify policy management, you can merge these multiple device policies into a single policy that you install on several devices at one time. For details, see “Merging Policies” on page 260.

Assigning a Policy to a Device

After you have created a firewall policy, you must assign that policy to a device. Assigning a policy to a device links the device to that policy, enabling 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 firewall policy to control multiple NetScreen FW/VPN devices. Each firewall rule in a policy contains an Install On column that specifies the devices the rule is applied to. This means that you can assign a 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 policy can be active on the device. When you update a device configuration, Security Manager installs the active policy on the NetScreen FW/VPN device. By default, 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.
CONFIGURING FIREWALL RULES

A firewall policy controls traffic flow on your network, from one network component to another network component. To do this, the firewall policy 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 will pass through. These areas include the network components that originate and receive the traffic, and the firewall zones the traffic passes through.

The Match columns of a firewall rule are required:

- 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 remaining columns are optional.

Defining Match

The following sections detail the Match columns of a firewall policy.

Source & Destination Zones

In the Zone-Specific 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 NetScreen FW/VPN device before you can create a policy 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 FW/VPN 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.

The Global Rulebase does not contain source and destination zone columns. Because global rules permit or deny traffic flow between all zones on the FW/VPN device, both the source and destination zones are global and so are not displayed.

Source & Destination Address Objects

You create firewall rules to enable traffic to flow between two network components. In the Security Manager system, address objects are used to represent the components on your network: hosts, networks, servers, etc. When you add the address object to the policy, you assign it to a security zone on your NetScreen FW/VPN device.

You must create Address Objects for the network components that originate and receive the traffic before you can create a firewall policy to control traffic between those components.
Example: 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 object that represents your trusted network. Your rule is similar to the example below:

<table>
<thead>
<tr>
<th>Match</th>
</tr>
</thead>
<tbody>
<tr>
<td>From Zone</td>
</tr>
<tr>
<td>![untrust]</td>
</tr>
</tbody>
</table>

To create a broader policy 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 FW/VPN 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: 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:

<table>
<thead>
<tr>
<th>Match</th>
</tr>
</thead>
<tbody>
<tr>
<td>From Zone</td>
</tr>
<tr>
<td>![Marketing]</td>
</tr>
</tbody>
</table>

The more specific you are in defining the source and destination address in a firewall rule, the better your firewall performs.

**Services**

Services are application layer protocols that define how data is structured as it travels across the network. In 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. Security Manager includes services that use TCP, UDP, RPC, and ICMP transport layer protocols.

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.
Configuring Firewall Rules

Example: 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:

<table>
<thead>
<tr>
<th>Match</th>
</tr>
</thead>
<tbody>
<tr>
<td>From Zone</td>
</tr>
<tr>
<td>trust</td>
</tr>
</tbody>
</table>

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: 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. 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:

<table>
<thead>
<tr>
<th>Match</th>
</tr>
</thead>
<tbody>
<tr>
<td>From Zone</td>
</tr>
<tr>
<td>trust</td>
</tr>
</tbody>
</table>

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 5.0 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 5.0 devices. For details, see “ScreenOS 5.0 Options” on page 251.

Defining Actions

You can specify the action that your NetScreen FW/VPN 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 in your firewall policy:

- **Permit.** Your NetScreen FW/VPN device permits the traffic to pass through firewall to its destination address.
- **Deny.** You NetScreen FW/VPN device does not permit the traffic to pass through the firewall, and drops all associated packets.

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 Attack Protection to detect attacks in permitted traffic.

**Note:** For firewall rules, the VPN action to “tunnel” is not available.

### Selecting Devices

In the install on column, select the device/s that receive and use this rule. You can select multiple NetScreen FW/VPN devices on which to install the firewall rule.

After you have created the policy and assigned the policy to a device, Security Manager only installs the rule on the devices specified in the Install Column of the rule, enabling you to use a single firewall policy for multiple NetScreen FW/VPN devices.

### Configuring Rule Options

Rule options enable you to configure additional protection mechanisms (such as AntiVirus or Deep Inspection) as well as logging, traffic shaping, NAT, and other miscellaneous features.

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 FW/VPN device to translate the IP address of incoming or outgoing traffic so that the packets are routable on the network.

#### Edit Source NAT

You can configure the NetScreen FW/VPN 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 NetScreen FW/VPN device, select Use Interface.

#### Edit Destination NAT

You can configure NetScreen FW/VPN devices running ScreenOS 5.0 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 NetScreen FWVPN 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 Chapter 4, “Configuring Devices”. For details on configuring NAT objects, see Chapter 7, “Configuring Objects”.

### Configuring Traffic Shaping

You can 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 NetScreen FW/VPN device handles the matching network traffic that exceeds the defined maximum bandwidth.

To set the minimum, or guaranteed bandwidth that is available to matching network traffic, enter the number of kilobits per second (kbps). This setting determines the minimum amount of throughput for the rule. The NetScreen FW/VPN device automatically passes matching traffic that has less than this throughput.

To set the maximum bandwidth available to the matching traffic, enter the number of kilobits per second (kbps). This setting determines the maximum amount of throughput for the rule. The NetScreen FW/VPN device throttles and drops matching traffic that has more than this throughput.

**Note:** NetScreen recommends that you do not set the maximum bandwidth to less than 10 kbps. Your NetScreen FW/VPN device might drop packets or the source address might attempt to resend the traffic repeatedly.

For matching traffic that falls between the guaranteed and maximum settings, your NetScreen FW/VPN device passes traffic based on the priority setting.

### Setting Priority

You can set a priority for each firewall rule in your policy. Your NetScreen FW/VPN 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.
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 the eight NetScreen priority levels to the DiffServ system: Priority 0 is the highest priority, and priority 7 is the lowest priority.

**Note:** 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. To change the default mappings between NetScreen priority levels and the DiffServ system, see the ScreenOS Concepts & Examples Guide 5.0.

### Enabling Logging & Counting

A good firewall 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 policy to log everything. You can choose to simply log the security event and create log entries with event information that you can view real-time in the Log Viewer. For more critical events you might want to be notified immediately by email or set an alert to appear in the log entry. Your goal is to fine-tune the notifications in your policy to your individual security needs.

### Configuring Logging

To log an event for a rule, enable logging. Each time your NetScreen FW/VPN device matches network traffic to the rule, Security Manager creates a log entry that describes that event and displays it in the Log Viewer. Depending on your security needs, you might want Security Manager to provide additional notification when a rule is matched, such as the number of bytes in matching network traffic or the alerts triggered.

### Configuring Alerts

You can also configure alerts that notify you when the matching network traffic falls outside your predefined byte range. To set an alert, enable counting and specify the minimum and maximum byte thresholds for matching network traffic.

### Configuring Counting

You can count how many bytes the matching network traffic contains and view this information in other applications. You can count by bytes per second, Kilobytes per minute, or both.

### Configuring Alarms

You can configure the device to send an alarm when the matching network traffic exceeds a predefined number of bytes per second, number of Kilobytes per minute, or both. A value of 0 indicates that the alarm is disabled.

You must enable Counting to set an Alarm threshold.
**Miscellaneous**

The following sections detail the Miscellaneous rule options in a firewall policy.

**Schedule**

To control the time period that your NetScreen FW/VPN device applies the rule to your network traffic, you can define a schedule for the rule. If you define a schedule, the NetScreen FW/VPN 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 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 Chapter 7, “Configuring Objects”.

You can use schedules to control the flow of network traffic at a time-sensitive level, and also enhance your network security.

Example: 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**

NS-5XT and NS-5GT FW/VPN 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 5.0 Options**

For FW/VPN devices running ScreenOS 5.0, you can configure additional rule options.

- **Application.** You can configure the FW/VPN 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 NetScreen FW/VPN device correctly checks traffic.

- **URL Filtering.** If you are using an integrated WebSense system with a ScreenOS 5.0 device, you can enable URL filtering.
Section: Configuring Firewall Policies

Authentication
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.
  - Default Server.
  - Local Server.
- **Web Authentication.** Use for RAS users using HTTP to connect to the protected network.

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 FW/VPN device intercepts the request packet and responds with a login prompt for user credentials.
Configuring Firewall Rules

- 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 (e.g., 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 FW/VPN device responds with a login prompt for user credentials.

For more details on User Objects, see Chapter 7, “Configuring Objects”.

**AntiVirus**

To configure antivirus protection for a firewall rule:

- **None**. No antivirus protection enabled.
- **Use AV Objects**. Antivirus objects represent specific viruses. You can use a maximum of three antivirus objects in a firewall rule to detect viruses in traffic.

**Note:** If you select the option *Use AV Objects*, you **must** select at least one object from the AntiVirus object list. Selecting this option without selecting AV objects results in a policy validation error.

- **Use Scan Manager**. Scan Manager is an embedded scanning engine. To use Scan Manager, the NetScreen FW/VPN device you install the policy on must an NS-5GT or NetScreen-Hardware Security Client (NS-HSC) device running ScreenOS 5.0. If you install a policy that uses Scan Manager on a a different device, the device executes and processes traffic according to the rule, but does not detect viruses using the embedded scanning engine.

**Configuring Attack Protection**

The following sections detail the Attack Protection rule options in a firewall policy.

**Attacks**

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 against your network. Use attack objects in your firewall rule to detect intrusion attempts within permitted traffic. To use attack objects:

- The firewall action must be permit. You cannot detect attacks in traffic that the firewall denies.
- The NetScreen FW/VPN device you install the policy on must be running ScreenOS 5.0. If you install a policy that contains attack objects on a ScreenOS 4.0.x device, the device executes and processes traffic according to the rule, but does not detect application-level attacks.
**Protection Options**

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 log the event, or use all three methods.

You can tell the firewall which actions to perform against attacks that match rules in your firewall policy. For each attack that matches a rule, actions respond to matching traffic using one of the following actions:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>The firewall takes no action against the connection.</td>
</tr>
<tr>
<td>ignore</td>
<td>The firewall ignores the remainder of a connection after an Attack group is matched.</td>
</tr>
<tr>
<td>drop packet</td>
<td>The firewall 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.</td>
</tr>
<tr>
<td>drop connection</td>
<td>The firewall 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 firewall closes the connection and sends a RST packet to both the client and the server.</td>
</tr>
<tr>
<td>close client</td>
<td>The firewall closes the connection to the client, but not to the server.</td>
</tr>
<tr>
<td>close server</td>
<td>The firewall closes the connection to the server, but not to the client.</td>
</tr>
</tbody>
</table>

**Attack Severity**

Each attack object has a default severity level of info, warning, minor, major, critical. To override the default severity level for an attack object in your rule, select a different severity level.

**Deep Inspection Alert**

This option sets an alert on an event log entry for matching traffic. If your FW/VPN device matches network traffic to an attack object in the rule, Security Manager creates an event log entry that describes that attack (direction, service, and Attack object) and displays an alert in the Log Viewer.

This option is ON by default.

**Comments**

Enter comments, if desired.
VALIDATING FIREWALL POLICIES

You should validate a firewall policy to identify potential problems before you install it. Common problems include:

- **Rule Duplication.** Occurs when one or more rules in the firewall 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 On column.

Security Manager contains a Policy Validation tool to help you locate additional problems, such as rule shadowing and unsupported options.

**Note:** NetScreen highly recommends that you validate a policy before installing. A policy that has internal problems can leave your network vulnerable.

Using the Policy Validation Tool

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 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:** To use the Policy Validation tool to validate a policy, you must first assign the policy to a device.

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 NetScreen FW/VPN device. To correct, return to the rule that is shadowing and modify or delete it. 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 5.0 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:

<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, HTTP</td>
</tr>
<tr>
<td>untrust</td>
<td>any</td>
<td>dmz</td>
<td>Web Server</td>
<td>HTTP, 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 5.0 device passes.

### Unsupported Options

Policy Validation can also identify unsupported options in your firewall policy. Because different NetScreen FW/VPN devices and system 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). Will be trimmed before an Update Device.
- Destination NAT Options not available on 4.0 devices. Will be trimmed before an Update Device.
- Antivirus Option not available on 4.0 devices. Will be trimmed before an Update Device.
- Deep Inspection Option not available on 4.0 devices. Will be trimmed before an Update Device.
- 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 NetScreen FW/VPN device in the Install On column of the rule, policy validation displays an information message that describes the unsupported feature.

*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 & Updating Firewall Policies

After you have successfully verified your policy, you can install it on your NetScreen FW/VPN devices.

Before Installing Policies

Before you install a policy, ensure that you have:

- **Assigned the policy to your devices.** After you have created a firewall 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 Security Manager to install the policy on that device.
- **Selected the correct devices for the Install On column of each rule.** A NetScreen FW/VPN device can only use one policy at a time; when you install a new policy, it overwrites all existing policies on the NetScreen FW/VPN device.
- **Configured rules in the Zone-Specific rulebase and Global rulebase correctly.** The management system installs rules from both rulebases on the specified device—global rules first, then zone rules.
- **Configured the VPN rules or VPN links in the policy correctly.** The management system installs all rules in the policy, including firewall rules, VPN rules, and VPN links.
- **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.

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

When you install a policy, Security Manager installs the rules in the policy on the NetScreen FW/VPN 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 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 5.0 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.
For details on the device ADM and DM, see the Chapter 6, “Managing Devices”.

**Updating Policies**

To install a policy, 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, and click OK.

The Job Manager task window appears and displays the progress of the policy installation. After the task 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 & POLICIES

Managing rules and policies for multiple firewalls can seem daunting at first. Take some time to carefully design your policies to make them efficient. Because a device can have only one policy installed at a time, you must include all rules for that device in one policy. Policies are listed alphabetically.

Using Zone Exceptions

A zone exception is a powerful tool that can help reduce the number of firewall rules in your policy while maintaining the same functionality. For devices that use more complicated and specific firewall rules, create a policy for each device and build specific rules for that device. Zone exceptions add flexibility to your firewall rules, enabling you to include more devices in a single rule.

Using Zone Filters

Filter on From and To Zones to see rules between zones.

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, & 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 firewall 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.
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 policy, but displays a gray diagonal stripe to indicate that it has been disabled. While the rule is disabled, 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.

Merging Policies

When you import policies from a single managed device, those policies appear in 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 firewall policy is a single statement that defines a source, destination, zone, direction, and service. In Security Manager, those same statements are known as firewall rules, and a firewall policy is a collection of firewall rules.

To simplify policy management and maintenance, you can merge two policies into a single 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).

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 in firewall policies (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 NetScreen FW/VPN 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 policy that contains both source and target rules, 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. Security Manager does not collapse rules that contain different zones, or rules that refer to unique VPNs.

You can merge any two FW/VPN policies. To access the Policy Merge tool, select the Firewall Policies module, then use the menu bar to select Tools > Policy Merge. See the Online Help for details.
### Example: Policy Merge

Policy A contains the following rules:

<table>
<thead>
<tr>
<th>Rule</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Install On</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1.1.1.1</td>
<td>2.2.2.2</td>
<td>FTP</td>
<td>NS-204</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>3.3.3.3</td>
<td>4.4.4.4</td>
<td>HTTP</td>
<td>NS-500</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>5.5.5.5</td>
<td>6.6.6.6</td>
<td>Telnet, ICMP</td>
<td>NS-5GT</td>
<td></td>
</tr>
</tbody>
</table>

Policy B contains the following rules:

<table>
<thead>
<tr>
<th>Rule</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Install On</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1.1.1.1</td>
<td>2.2.2.2</td>
<td>FTP</td>
<td>NS-5GT</td>
<td>NS-5XG</td>
</tr>
<tr>
<td>2</td>
<td>3.3.3.3</td>
<td>4.4.4.4</td>
<td>HTTP</td>
<td>NS-208</td>
<td>NS-204</td>
</tr>
<tr>
<td>3</td>
<td>5.5.5.5</td>
<td>6.6.6.6</td>
<td>Telnet, ICMP</td>
<td>NS-5400</td>
<td></td>
</tr>
</tbody>
</table>

When Policy A (source policy) is merged above Policy B (target policy), Security Manager first copies all rules from Policy A and pastes them above the rules in Policy B (this screen is not shown in Security Manager):

<table>
<thead>
<tr>
<th>Rule</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Install On</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1.1.1.1</td>
<td>2.2.2.2</td>
<td>FTP</td>
<td>NS-204</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>3.3.3.3</td>
<td>4.4.4.4</td>
<td>HTTP</td>
<td>NS-500</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>5.5.5.5</td>
<td>6.6.6.6</td>
<td>Telnet, ICMP</td>
<td>NS-5GT</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>1.1.1.1</td>
<td>2.2.2.2</td>
<td>FTP</td>
<td>NS-5GT</td>
<td>NS-5XG</td>
</tr>
<tr>
<td>5</td>
<td>3.3.3.3</td>
<td>4.4.4.4</td>
<td>HTTP</td>
<td>NS-208</td>
<td>NS-204</td>
</tr>
<tr>
<td>6</td>
<td>5.5.5.5</td>
<td>6.6.6.6</td>
<td>Telnet, ICMP</td>
<td>NS-5400</td>
<td></td>
</tr>
</tbody>
</table>

Finally, Security Manager merges the matching values in the columns to create a single, simplified policy:

<table>
<thead>
<tr>
<th>Rule</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Install On</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1.1.1.1</td>
<td>2.2.2.2</td>
<td>FTP</td>
<td>NS-204</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>3.3.3.3</td>
<td>4.4.4.4</td>
<td>HTTP</td>
<td>NS-500</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>5.5.5.5</td>
<td>6.6.6.6</td>
<td>Telnet, ICMP</td>
<td>NS-5GT</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>1.1.1.1</td>
<td>2.2.2.2</td>
<td>FTP</td>
<td>NS-5GT</td>
<td>NS-5XG</td>
</tr>
<tr>
<td>5</td>
<td>3.3.3.3</td>
<td>4.4.4.4</td>
<td>HTTP</td>
<td>NS-208</td>
<td>NS-204</td>
</tr>
<tr>
<td>6</td>
<td>5.5.5.5</td>
<td>6.6.6.6</td>
<td>Telnet, ICMP</td>
<td>NS-5400</td>
<td></td>
</tr>
<tr>
<td>Rule</td>
<td>Source</td>
<td>Destination</td>
<td>Service</td>
<td>Install On</td>
<td>Comments</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>-------------</td>
<td>------------</td>
<td>------------</td>
<td>----------</td>
</tr>
<tr>
<td>2</td>
<td>3.3.3.3</td>
<td>4.4.4.4</td>
<td>HTTP</td>
<td>NS-500</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>NS-208</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>NS-204</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>5.5.5.5</td>
<td>6.6.6.6</td>
<td>Telnet, ICMP</td>
<td>NS-5GT</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>NS-5400</td>
<td></td>
</tr>
</tbody>
</table>
In This Chapter:

- About VPNs
- Planning for Your VPN
- Preparing VPN Components
- Creating VPNs with VPN Manager
- VPN Manager Examples
- Creating Device-Level VPNs

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 Online Help Topic “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.
About VPs

With Security Manager, you can use basic networking principles and your NetScreen FW/VPN devices to create VPs that connect your headquarters with your branch offices and your remote users with your protected networks.

Security Manager supports tunnel and transport modes for AutoKey IKE, Manual Key, L2TP, and L2TP-over-AutoKey IKE VPs in policy or route-based configurations. You can create the VP at the system-level or device-level:

- **System-Level VPN (VP 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 NetScreen FW/VPN device, then add VPN rules to a Firewall Policy to create a policy-based VPN or configure routes on each FW/VPN device to create a route-based VPN.

Creating System-Level VPs with VP Manager

For AutoKey IKE and L2TP VPs, create the VPN at the system-level using VP Manager. VP Manager supports:

- **AutoKey IKE VPs** 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 VPs** and **L2TP RAS VPs** that 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 VPs.
- **Compact and Expanded Views**. Choose the Compact (default) or Expanded view to create your VPN. Both views offer the same configuration options.
- **Iutogenerated Tunnels**. Create tunnel interfaces on each route-based VPN member automatically. Use the device tunnel summary to review all autogenerated tunnels in the VPN.
- **Iutogenerated VPN Rules**. Create all VPN rules with a single click. 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 firewall policy.

To view all VPs created with VP Manager, select VP Manager in the navigation tree. A list of saved VPs appears in the main display area in table format. You can add and delete VPs from this view.

VP Manager does not support Manual Key VPs; to create a Manual Key VPN in 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 FW/VPN device.

After you have configured the VPN on each FW/VPN device in the VPN, add VPN rules to a Firewall 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

Security Manager supports all possible VPN configurations that are supported by the CLI and 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

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?
- **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 & Topology

You can use a VPN to connect:

- **FW/VPN devices.** Create a VPN between two or more FW/VPN devices to establish secure communication between separate networks.
- **Network components.** Create a VPN between a two or more network components to establish secure communication between specific machines.
- **Remote users.** Create a VPN between a user and a FW/VPN device to enable secure access to protected networks.

\[\text{Note: In Security Manager, remote users are known as remote access service (RAS) users.}\]

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 FW/VPN device.

Using Network Address Translation (NAT)

Network Address Translation (NAT) maps private IP addresses to public, Internet-routable IP addresses. Because your FW/VPN 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 FW/VPN device translates the unregistered IP address in the outbound data packets to the registered address of the FW/VPN device. The FW/VPN 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 FW/VPN device or RAS user that connects to a central FW/VPN device.

- **Advantages:** Simple, easy to configure.
- **Disadvantages:** The central FW/VPN 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 & Spoke

In a hub and spoke VPN, multiple FW/VPN 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 NetScreen FW/VPN 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 FW/VPN 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
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. Security Manager provides two tunneling protocols, IPSec and L2TP, as detailed in the following sections.

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 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. Security Manager supports the following IPSec data protection services for VPNs.

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).

- **Pre-shared Secret.** 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 Chapter 4, “Configuring Devices”.

Authentication only authenticates the data; it does not encrypt the data in the VPN. To ensure privacy, you must encrypt the data using ESP.
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. 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 NetScreen FW/VPN devices to inspect every IPsec packet to see if the packet has been received before—if packets arrive outside a specified sequence range, the NetScreen FW/VPN device rejects them.
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 routable, UDP packet. L2TP VPNs supports remote access service users using Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP) authentication.

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 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.
Policy-Based

A policy-based VPN tunnels traffic between two FW/VPN devices, or between one FW/VPN device and a remote user. Each time a NetScreen FW/VPN device detects traffic that matches the from zone, source, to zone, destination, and service in the VPN rule, Security Manager creates a VPN tunnel to encrypt, authenticate, and send the data to the specified destination. When no traffic matches the VPN rule, 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 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.

An example is shown below:

Route-Based

Like a policy-based VPN, a route-based VPN tunnels traffic between two FW/VPN devices, or between one FW/VPN 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 FW/VPN 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 FW/VPN 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.
Planning for Your VPN

An example is shown below:

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.

Members & 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 & 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.

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.
Security Protocol (Encryption & 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.

VPN Manager or Device-Level?

How do you want to create the tunnel? Using VPN Manager or configuring each device?

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:

- Use an Autokey IKE VPN 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)

- Use an Autokey IKE RAS VPN to authenticate and encrypt traffic between remote users and protected resources. An Autokey IKE RAS VPN supports:
  - Policy-based VPNs
  - ESP and AH Authentication
  - ESP AutoKey IKE Encryption
  - IP traffic
  - Remote access users
• Use an **L2TP RAS VPN** 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

• Use an **L2TP over Autokey IKE RAS VPN** 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

*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:

- **Basic VPN components**
- **Required Policy-based VPN components**
- **Required Route-based VPN components**
- **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 Online Help Topic “VPNs”.

Basic VPN Components

To create any type of VPN, ensure that all FW/VPN devices you want to use in the VPN are managed by Security Manager and configured correctly.

- **Devices.** Add the FW/VPN devices you want to include in the VPN to 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 Chapter 3, “Adding Devices”.

- **Zones.** Configure each FW/VPN 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 4, “Configuring Devices”.

Required Policy-Based VPN Components

A policy-based VPN requires several components:

- Address Objects
- Protected Resources
- NAT Objects
- User Objects

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 Chapter 7, “Configuring Objects”.

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 FW/VPN 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 FW/VPN device that protects them.

An example is show below:

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, as shown below:

When creating protected resources:

- To protect multiple network components that are accessible by the same FW/VPN 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 FW/VPN 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 FW/VPN device but specify a different service object.

If you change the FW/VPN device that protects a resource, Security Manager removes the previous FW/VPN device from all affected VPNs and adds the new FW/VPN device. However, Security Manager does not configure the VPN topology for the new FW/VPN—you must reconfigure the topology to include the new device manually.

For more details on creating protected resources, see Chapter 7, “Configuring Objects”.

### 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 FW/VPN 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 (a global DIP represents multiple device-specific DIPs, etc.) 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 Chapter 7, “Configuring Objects”.

### Configuring Remote Access Service (RAS) Users

For VPNs that support RAS users, you must create a User Object to represent each user. Security Manager supports two types of users:

- **Local Users.** A local user has an account on the FW/VPN device that guards the protected resources in the VPN. When a local user attempts to connect to a protected resource, the FW/VPN 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 FW/VPN device forwards the request to the authentication server for authentication.
Authentication 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 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 FW/VPN device configuration, not in the Object Manager. For details on creating manual key users, see “Adding XAuth Users” on page 331.

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 FW/VPN 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 NetScreen platform).

For details on group IKE IDs, see the ScreenOS 5.0 Concepts & Examples Guide.

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 & Tunnel Zones

A VPN requires a physical or virtual interface on the FW/VPN device, and each NetScreen FW/VPN 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 the NetScreen ScreenOS 5.0 Concepts & Examples Guide.

Configuring Static & Dynamic Routes

A FW/VPN device must know the path, or route, between each protected resource or FW/VPN 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, NetScreen 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 Chapter 4, “Configuring Devices”.

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 the NetScreen ScreenOS 5.0 Concepts & Examples Guide.

Configuring Static & Dynamic Routes

A FW/VPN device must know the path, or route, between each protected resource or FW/VPN 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, NetScreen 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 Chapter 4, “Configuring Devices”.
Optional VPN Components

In any type of VPN, you can also use two optional components:

- Authentication Server
- Certificate & 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 Chapter 7, “Configuring Objects”.

Creating Certificate Objects

To authenticate external devices, use a Group IKE ID to authenticate multiple RAS users, or provide additional authentication for the FW/VPN 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:

- A local certificate for each FW/VPN 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 FW/VPN 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 a 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 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 Chapter 4, “Configuring Devices”.

### 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 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 Chapter 7, “Configuring Objects”.

### 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 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 Chapter 7, “Configuring Objects”.

### Creating PKI Defaults

You can configure default PKI settings for each FW/VPN 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 Chapter 4, “Configuring Devices”.

Chapter 9 Configuring VPNs
Creating VPNs with VPN Manager

Configuring a VPN using VPN Manager is an eight stage process:

1. Adding the VPN
2. Configuring Members (policy-based, RAS users, routing-based)
3. Configuring Topology (AutoKey IKE only)
4. Configuring Gateways
5. Configuring IKE
6. Autogenerating the VPN
7. Configuring Overrides
8. 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 Online Help Topic “VPNs”.

Adding the VPN

From the menu bar, click VPN Manager > New and select the VPN type:

- **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.
- **Use an AutoKey IKE RAS VPN** 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.
- **Use an L2TP RAS VPN** to connect L2TP RAS users and protected resources without encryption.
- **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 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.

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, FW/VPN 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 Chapter 7, “Configuring Objects”.

After you have added the protected resources, you can configure NAT and/or L2TP settings on the FW/VPN 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-routable 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 FW/VPN 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 FW/VPN 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 FW/VPN device. (This DIP pool must include IP addresses that are routable on your internal network.)

For details on configuring DIP objects, see Chapter 7, “Configuring Objects”.

- **Configure Tunnel Interface & Zone.** You can bind the VPN tunnel to a tunnel interface or tunnel zone to increase the number of available interfaces in the FW/VPN device.

**Note:** If the FW/VPN device is running ScreenOS 5.0 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 & Tunnel Zones” on page 280 and Chapter 4, “Configuring Devices”.

**Note:** In VPN Manager, you cannot assign multiple VPN tunnels to a single interface. However, you can do this at the device level.

- **Tunnel Zone.** Select a pre-configured tunnel zone on the FW/VPN devices to bind the VPN tunnel directly to the tunnel zone. The tunnel zone must include one or more numbered tunnel interfaces; when the FW/VPN 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 FW/VPN devices to bind the VPN tunnel to the tunnel interface. The FW/VPN devices route all VPN traffic through the tunnel interface to the protected resources.

**Configure MIP, VIP, & 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 FW/VPN 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 FW/VPN device. (This DIP pool must include IP addresses that are routable 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 FW/VPN 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 FW/VPN 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.

**Note**: To use the default authentication server for L2TP users, add the users to the device first.

### 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 Chapter 7, Configuring Objects.

### 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 FW/VPN 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 NetScreen FW/VPN devices to route traffic through these tunnel interfaces. For details on creating routes, see Chapter 4, “Configuring Devices”.

Click the FW/VPN devices link to display the route-based member selection dialog box.
• **Configure Tunnel Interface Settings.** Select a Primary Zone and Secondary Zone for each FW/VPN device. The selected zone passes VPN traffic through the FW/VPN 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 FW/VPN device, VPN traffic automatically uses the Secondary Zone.
  - You can specify unique tunnel interface zones for each route-based member in the Overrides area. For details, see “Configuring Overrides” on page 295.

• **Configure Members.** Click the Edit icon to select the predefined FW/VPN devices you want to include in the VPN. 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 FW/VPN device that protects a resource, Security Manager removes the previous FW/VPN device from all affected VPNs and adds the new FW/VPN device. However, Security Manager does not configure the VPN topology for the new FW/VPN—you must reconfigure the topology to include the new device manually.

### Defining Topology

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.

• **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 & 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 & 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 FW/VPN device in the VPN. The Termination Points tab displays the default termination points for the VPN. A termination point is the interface on a FW/VPN device that sends and receives VPN traffic to and from the VPN tunnel, and is typically in the Untrust zone. Each VPN member (the FW/VPN devices included as routing-based members and/or as protected resources for policy-based members) has a default termination interface.

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 FW/VPN devices wait between sending hello pulses.
- **Reconnect**. Enter the maximum number of seconds the FW/VPN devices wait for a reply to the hello pulse.
- **Threshold**. Enter the number of seconds that the FW/VPN 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 FW/VPN 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 NetScreen FW/VPN 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.

- **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 in the FW/VPN device configuration.

- **Use XAuth Server** when the remote gateway is a FW/VPN 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 Chapter 7, “Configuring Objects”.
  - 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.

- **Use XAuth Client** 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.

- **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:

- **Use Preshared Key** if your VPN includes NetScreen FW/VPN 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, click Generate Key.
  - To use a predefined value for the key, enter a value for the Preshared Key

  **Note:** Using a random key can generate CLI commands in excess of 255 characters, which exceeds ScreenOS limits and might not be accepted by the NetScreen FW/VPN device during update. To reduce the key size, shorten the autogenerated key value by deleting characters.

- **Use PKI** 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 Chapter 7, “Configuring Objects”.

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 Chapter 7, “Configuring Objects”.

If your VPN includes only NetScreen FW/VPN devices, you can specify one predefined or custom proposal that 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 FW/VPN 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 279. For details on determining the ASN1-DN container and wildcard values for Group IKE IDs, see the NetScreen ScreenOS 5.0 Concepts & 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.
Creating VPNs with VPN Manager

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 NetScreen FW/VPN devices inspect every IPSec packet to see if the packet has been received before—if packets arrive outside a specified sequence range, the NetScreen FW/VPN device rejects them.
- **IPSec Mode.** Configure the mode:
  - Use tunnel mode for IPSec. Before an IP packet enters the VPN tunnel, 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. 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 NetScreen FW/VPN 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 NetScreen FW/VPN 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:
Chapter 9 Configuring VPNs

- 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 NetScreen ScreenOS 5.0 Concepts & Examples Guide. For details on VPN Monitor (in Realtime Monitor) in NetScreen-Security Manager, see Chapter 10, “Monitoring”.

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 Chapter 7, “Configuring Objects”.

If your VPN includes only NetScreen FW/VPN devices, you can specify one predefined or custom proposal that 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 the VPN

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, Security Manager generates the VPN rules that control traffic between policy-based VPN members, and edits the device configuration (gateways, security parameters, etc.) of each VPN member to support the VPN.

Autogeneration does not:

- Insert the VPN rules into a firewall policy. After you have reviewed the VPN rules and made any necessary overrides, you must manual insert the VPN rules (known as a VPN link) into a firewall policy. For details, see “Adding the VPN Link” on page 297.
- 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 firewall 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, 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 Security Manager window, using the same row and column format as in the Policy Manager.

**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 Chapter 8, “Configuring Firewall Policies”.
Editing Device Configuration

For all VPNs, you can edit the device configuration for each VPN member. The device configuration displays the interfaces, gateways, etc. for each individual device.

Interface

For route-based and mixed-mode VPNs, this displays the tunnel interfaces 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.

AutoKey IKE VPN

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.

Gateway

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.

VPN Group

For all VPNs, this displays VPN groups.

L2TP

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 are ready to add the VPN rules to a firewall policy and install that policy on your managed devices. To add the VPN rules, you must create a VPN link between the firewall policy and VPN. In Policy Manager, you create this link by inserting a VPN link in the firewall policy; this links points to the VPN rules that exist in the VPN in VPN Manager.

To create a VPN link, in Policy Manager, select an existing firewall policy (or create a new firewall 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

You can edit a VPN created with VPN Manager by changing:

- Protected Resources
- VPN Configuration
- Overrides

Editing VPN Protected Resources

If you make changes to a protected resource object that is used in a VPN, Security Manager automatically generates new configuration and propagates your changes to all affected FW/VPN devices. If you change the FW/VPN device that protects a resource, Security Manager removes the previous FW/VPN device from all affected VPNs and adds the new FW/VPN device.

However, Security Manager does not configure the VPN topology for the new FW/VPN—you must reconfigure the topology to include the new device manually.

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.

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:

- AutoKey IKE, Policy-Based Site-to-Site VPN
- AutoKey IKE RAS, Policy-Based VPN
- AutoKey IKE, Route-Based Site-to-Site VPN

The following sections provide step-by-step instructions on creating each type of VPN.

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 NetScreen FW/VPN 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.

Step 1: Create VPN Components

To create an AutoKey IKE, Site-to-Site VPN, create the following VPN components:

- NetScreen FW/VPN Devices
- Address Objects
- Protected Resources

The following sections detail how to create each component.
Create the NetScreen FW/VPN Devices

Add the Tokyo and Paris NetScreen FW/VPN devices (for details on adding devices, see Chapter 3, “Adding Devices”):

- 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.
- 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.

Create the Address Objects

Create the Address Objects that you will use to create Protected Resources (for details on creating or editing Address Objects, see Chapter 7, “Configuring Objects”). If you imported a NetScreen FW/VPN device, the address book objects configured on that device are automatically imported as Address Objects into the Security Manager UI.

To add the Tokyo Trust LAN (10.1.1.0/24) as an network Address Object:

1. In Address Objects, click the Add icon and select Network.
2. Configure the object as shown below:

![Network Object Configuration](image)

3. Click OK to save the object and return to Object Manager.
To add the Paris Trust LAN (10.2.2.0/24) as a network Address Object:

1. In Address Objects, click the Add icon and select Network.
2. Configure the object as shown below:

![Network Configuration](image.png)

3. Click OK to save the object and return to Object Manager.

Create the Protected Resources

Create the Protected Resources to represent the source and destination points of the VPN. (for details on creating or editing Protected Resources, see Chapter 7, “Configuring Objects”).

To create the Tokyo Protected Resources object:

1. In Protected Resources (under VPN Manager), click the Add icon.
2. Configure the object as shown below:

![Protected Resource Configuration](image.png)

3. Click OK to save the object and return to VPN Manager.
To create the Paris Protected Resources object:

1. In Protected Resources (under VPN Manager), click the Add icon.
2. Configure the object as shown below:

![Protected Resource window]

3. Click OK to save the object and return to VPN Manager.

**Step 2: Create the VPN**

1. In the Navigation Tree, double-click VPN Manager, right-click VPNs and select **AutoKey IKE VPN**. The New AutoKey IKE VPN dialog box appears.
2. In Name, enter **Tokyo-Paris Policy-Based VPN**.
3. Select **Enable**.
4. In **Termination Point**, select **Untrust**.
5. Click **OK** to save the VPN and return to VPN Manager.

**Step 3: Configure the VPN**

1. In VPN Manager, select the **Tokyo-Paris Policy-Based VPN**. The VPN appears in the main display area.
2. Configure the policy-based members:
   a. Select the **Protected Resources** link to display the Protected Resources list.
b. Select the following Protected Resources, as shown below:

![Protected Resource]

- Chicago Corporate Trusted LAN
- My Protected Resources
- Paris Protected Resources
- Tokyo Protected Resources

c. Click OK to return to the main display area.

3. 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.
   c. In the Mains window, select the following NetScreen FW/VPN devices, as shown below:

![Topology]

- Paris
- Tokyo

d. Click OK to return to the Topology dialog box, then click OK to return to the main display area.
4. 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, as shown below:

   ![Termination Point Dialog Box](image)

   - Firewall Device | Termination Interface
   - Paris          | ethernet3
   - Tokyo         | ethernet3

c. Click **OK** to return to the main display area.

5. 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:

   ![Gateway Parameters](image)

   - Preshared Key/RSA/DSA: **PKI Information**
   - Peer Type: **XS09-SIG**
   - All CA in Trusted CA Certificate Store: **Peer CA Hash**
   - Phase 1 Proposals:
     - Security Level: **User-Defined**
       - rsa-g2-3des-sha

   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:

![AutoKey IKE VPN]

**Step 4: Add the VPN Link**

You must create a VPN link between the firewall policy and the VPN Manager autogenerated rules. You create this link by inserting a VPN link in the firewall policy; this links points to the VPN rules that exist in the VPN Manager.

To create a VPN link:

1. In Policy Manager, select an existing firewall policy (or create a new firewall policy). Right-click and select Add VPN link.
2. Select the **Tokyo-Paris Policy-Based VPN**.
3. 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.

**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 FW/VPN 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.

Step 1: Create VPN Components

To create an AutoKey RAS IKE, Site-to-Site VPN, create the following VPN components:

- NetScreen FW/VPN Devices
- Address Objects
- Protected Resources
- User Objects

The following sections detail how to create each component.

Create the NetScreen FW/VPN Device

Add the Chicago Corporate device (for details on adding devices, see Chapter 3, “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.

Create Address Objects

Create the Address Objects that you will use to create Protected Resources (for details on creating or editing Address Objects, see Chapter 7, “Configuring Objects”).
To add the Chicago Corporate Trusted LAN (10.1.1.0/24) as an network Address Object:

1. In Address Objects, click the Add icon and select **Network**.
2. Configure the object as shown below:

3. Click OK to save the object and return to Address Objects.

To add the UNIX Server (10.1.1.5) as a host Address Object:

1. In Address Objects, click the Add icon and select **Host**.
2. Configure the object as shown below:

3. Click OK to save the object and return to Address Objects.
Create Protected Resources

Create a Protected Resource to represent the destination point of the VPN (for details on creating Protected Resources, see Chapter 7, “Configuring Objects”).

To create the Chicago Corporate Trusted LAN Protected Resources object:

1. In Protected Resources (under VPN Manager), click the Add icon.
2. Configure the object as shown below:

   ![New Protected Resource Window]

   - Name: Chicago Corporate Trusted LAN
   - Color: green
   - Service Object: any
   - Server/Client: Server
   - Network Object: UNIX Server
   - Comment: UNIX file server access
   - Security Gateway Device: Zone
     - Chicago Corporate: trust

3. Click OK to save the object and return to VPN Manager.

Create the User Object

Create a Local User Object to represent Wendy, the remote user (for details on creating or editing User Objects, see Chapter 7, “Configuring Objects”). Local User objects are authenticated with the local Security Manager database.
To add Wendy as a User Object:

1. In User Objects, select Local User Objects. In the main display area, click the Add icon and select Local.
2. Configure the object as shown below:

![Local User Object Configuration]

- Name: wparker
- Color: yellow
- Comment: chicago se
- Enable: checked
- XAuth: IKE, Auth, L2TP
- Password: Set Password...
- IKE Share Limit: 1
- User FQDN: wparker@abc.com

3. Click OK to save the object and return to Local User Objects.

**Step 2: Create the VPN**

1. In the Navigation Tree, double-click VPN Manager, right-click VPNs and select AutoKey IKE RAS VPN. The New AutoKey IKE RAS VPN dialog box appears.
2. In Name, enter UNIX Remote Access VPN.
3. Select Enable.
4. In Termination Point, select Untrust.
5. Click OK to save the VPN and return to VPN Manager.
Step 3: Configure the VPN

1. In VPN Manager, select the **UNIX Remote Access VPN**.
2. Configure the policy-based members:
   a. In the main display area, select the **Protected Resources** link.
   b. In the Protected Resources list, select the following Protected Resources, as shown below:

   ![Protected Resource List]

   c. Click **OK** to return to the main display area.
3. 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 zone interface) as shown below:

```
Termination Point

<table>
<thead>
<tr>
<th>Firewall Device /</th>
<th>Termination Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chicago Corporate</td>
<td>ethernet3</td>
</tr>
</tbody>
</table>
```

c. Click OK to return to the main display area.

4. 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” as shown below:

```
Remote User

[ ] Remote User
  [ ] wparker
```

c. Click Save to save your configuration changes to the VPN.

5. 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:

![VPN Manager Interface](image)

- **Properties**
  - Preshare Key/RSA/DSA
  - Generate Key

- **IKE IDs**
  - Preshared Key: 
  - Security Level: User-Defined

- **Phase 1 Proposals**
  - Security Level: User-Defined
  - pre-g2-3des-sha

- **User-Defined**

  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:

![VPN Manager Policy Rules](image)

---

**Step 4: Add the VPN Link**

You must create a VPN link between the firewall policy and the VPN Manager autogenerated rules. You create this link by inserting a VPN link in the firewall policy; this links points to the VPN rules that exist in the VPN Manager.
To create a VPN link:

1. In Policy Manager, select an existing firewall policy (or create a new firewall policy). Right-click and select Add VPN link.
2. Select the **UNIX Remote Access VPN**.
3. 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.

**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 NetScreen FW/VPN devices protecting the Tokyo and Paris offices. The Untrust zone interface for both NetScreen FW/VPN 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 proposals as predefined compatible.

### Step 1: Create VPN Components

To create an AutoKey IKE, Route-based, Site-to-Site VPN, create the following VPN components:

- **NetScreen FW/VPN Devices**
- **Address Objects**

The following sections detail how to create each component.
Add the NetScreen FW/VPN Devices

Add the Tokyo and Paris FW/VPN devices (for details on adding devices, see Chapter 3, “Adding Devices”):

- 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).
- 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.

Create the Address Objects

Create the Address Objects that you will use to create the VPN rule in your firewall policy (for details on creating VPN rules, see “Adding VPN Rules” on page 335). If you imported a NetScreen FW/VPN device, the address book objects configured on that device are automatically imported as Address Objects into the Security Manager UI.

To add the Tokyo Trust LAN (10.1.1.0/24) as an network Address Object:

1. In Address Objects, click the Add icon and select Network.
2. Configure the object as shown below:

   ![Network Configuration Window]

   - Name: Tokyo Trust LAN
   - IP Address: 10.1.1.0
   - Netmask: 24
   - Color: magenta
   - Comment: Tokyo Trust Zone

3. Click OK to save the object and return to Object Manager.
To add the Paris Trust LAN (10.2.2.0/24) as a network Address Object:

1. In Address Objects, click the Add icon and select **Network**.
2. Configure the object as shown below:

   ![Network Configuration](image)

   - **Name**: Paris Trust LAN
   - **IP Address**: 10.2.2.0
   - **Netmask**: 24
   - **Color**: Magenta
   - **Comment**: Paris Trust Zone

3. Click **OK** to save the object and return to Object Manager.

**Step 2: Create the VPN**

1. In the Navigation Tree, double-click VPN Manager, right-click VPNs and select **AutoKey IKE VPN**. The New AutoKey IKE VPN dialog box appears.
2. In Name, enter **Tokyo-Paris Route-Based VPN**.
3. Select **Enable**.
4. In **Termination Point**, select **Untrust**.
5. Click **OK** to save the VPN and return to VPN Manager.

**Step 3: Configure the VPN**

1. In VPN Manager, select the **Tokyo-Paris Route-Based VPN**.
2. Configure the route-based members:
   a. In the main display area, select the **FW/VPN Device** link (under Route-Based Configuration) to display the tunnel interface summary.
   b. Click the Add icon to display available FW/VPN devices.
c. Configure the route-based members as shown below:

![AutoKey IKE VPN dialog box]

```
Route Based Members
  - Chicago
  - NS-5GT
  - NS-5XT
  - NS-208A
  - Paris
  - Tokyo
  - test4444
```

d. Click OK to add the members and return to the tunnel interface summary, then click OK to return to the main display area.

3. 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.
c. In the **Mains** window, select the following NetScreen FW/VPN devices, as shown below:

![Topology window]

- **Hub**: Please select…
- **Supernet**: Please select…
- **Mains**:
  - Paris
  - Tokyo
- **Branches**:
  - Paris
  - Tokyo

![Termination Points window]

- **Termination Interface**:
  - Paris: ethernet3
  - Tokyo: ethernet3

d. Click **OK** to return to the Topology dialog box, then click **OK** to return to the main display area.

4. 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, as shown below:

   ![Termination Points window (details)]

   - **Firewall Device**
     - Paris: ethernet3
     - Tokyo: ethernet3

c. Click **OK** to return to the main display area.
5. 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:

   ![VPN Manager Examples](image)

   6. 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 FW/VPN device in the VPN, as shown below:

![VPN Manager Examples](image)

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 firewall policy that is installed on each VPN node. For details on creating firewall rules, see Chapter 8, “Configuring Firewall Policies”.

**Step 4: Create Routes**

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 Chapter 4, “Configuring Devices”). 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.

To configure the route on the Tokyo FW/VPN device:

1. 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.
2. 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 5.0.0 devices display both destination-based and source-based routing tables.
3. Configure a route from the untrust interface to the gateway, as shown below:

![Routing Table](image1.png)

4. Configure route from the trust zone to the tunnel interface, as shown below:

![Routing Table](image2.png)
Your routing table should appear as shown below:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Mask</th>
<th>Next Hop</th>
<th>Vsyst</th>
<th>Interface:</th>
<th>Gateway IP Address:</th>
<th>Metric:</th>
<th>Tag:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>0</td>
<td></td>
<td>...</td>
<td>ethernet3</td>
<td>1.1.1.250</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>10.2.2.0</td>
<td>24</td>
<td></td>
<td>...</td>
<td>tunnel.1</td>
<td>0.0.0.0</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

5. Click OK to save your changes to the virtual router, then click OK to save your changes to the Tokyo device.

To configure the route on the Paris FW/VPN device:

1. 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.

2. 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 5.0.0 devices display both destination-based and source-based routing tables.
3. Configure a route from the untrust interface to the gateway, as shown below:

![Routing Table](image1.png)

4. Configure route from the trust zone to the tunnel interface, as shown below:

![Routing Table](image2.png)
Your routing table should appear as shown below:

<table>
<thead>
<tr>
<th>IP Address / Mask</th>
<th>Next Hop</th>
<th>Vsys</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0 / 0</td>
<td>Interface: ethernet3&lt;br&gt;Gateway IP Address: 2.2.2.250&lt;br&gt;Metric: 1&lt;br&gt;Tag: ...</td>
<td></td>
</tr>
<tr>
<td>10.1.1.0 / 24</td>
<td>Interface: tunnel.1&lt;br&gt;Gateway IP Address: 0.0.0.0&lt;br&gt;Metric: 1&lt;br&gt;Tag: ...</td>
<td></td>
</tr>
</tbody>
</table>

5. Click OK to save your changes to the virtual router, then click OK to save your changes to the Paris device.
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 323.
- 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 331.
- 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 334.
- 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 335.

**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:

1. Configure Gateway
2. Configure Routes (Route-based only)
3. Configure VPN on the Device
4. Add VPN rules to Firewall Policy

**Configuring Gateways**

A gateway is an interface on your FW/VPN device that sends and receives traffic; a remote gateway is an interface on another device that handles traffic for that device. Each FW/VPN 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 FW/VPN 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 FW/VPN 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 FW/VPN device waits between sending hello pulses.
- **Reconnect.** Enter the maximum number of seconds the FW/VPN waits for a reply to the hello pulse.
- **Threshold.** Enter the number of seconds that the FW/VPN 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.

You do not need to enable NAT-T for your internal FW/VPN 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 NetScreen FW/VPN 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 279. For details on determining the ASN1-DN container and wildcard values for Group IKE IDs, see NetScreen ScreenOS 5.0 Concepts & 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.

- **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 >Default >Xauth settings.
- **Use XAuth Server** 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 Chapter 7, “Configuring Objects”.
  - **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 & Groups.** To authenticate XAuth RAS users using the authentication server, enable User or User Group and select a preconfigured user object.
- **Use XAuth Client** 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.
- **Use Bypass Authentication** to permit VPN traffic from this VPN member to pass unauthenticated by the Auth server.
Select the authentication method you want to use in the VPN:

- **Use Preshared Key** if your VPN includes NetScreen FW/VPN 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, click Generate Key.
  - To use a predefined value for the key, enter a value for the Preshared Key.

  **Note:** Using a random key can generate CLI commands in excess of 255 characters, which exceeds ScreenOS limits and might not be accepted by the NetScreen FW/VPN device during update. To reduce the key size, shorten the autogenerated key value by deleting characters.

- **Use PKI** 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 Chapter 7, “Configuring Objects”.

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 Chapter 7, “Configuring Objects”.

If your VPN includes only NetScreen FW/VPN devices, you can specify one predefined or custom proposal that 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 FW/VPN 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 Chapter 4, "Configuring Devices".

After you have configured the tunnel zone or interface on the FW/VPN 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 FW/VPN device uses to connect to the VPN, the IKE Phase 2 proposals used by that gateway, and how you want 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 NetScreen FW/VPN devices inspect every IPSec packet to see if the packet has been received before—if packets arrive outside a specified sequence range, the NetScreen FW/VPN device rejects them.
- **IPSec Mode.** Configure the mode:
  - Use tunnel mode for IPSec. Before an IP packet enters the VPN tunnel, 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. 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.
Creating Device-Level VPNs

**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 Chapter 7, “Configuring Objects”.

If your VPN includes only NetScreen FW/VPN devices, you can specify one predefined or custom proposal that 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 FW/VPN 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 & Tunnel Zones” on page 280 and Chapter 4, “Configuring Devices”:

- **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 FW/VPN device to bind the VPN tunnel to the tunnel interface. The FW/VPN device routes all VPN traffic through the tunnel interface to the protected resources.
- **Tunnel Zone.** Select a pre-configured tunnel zone on the FW/VPN device to bind the VPN tunnel directly to the tunnel zone. The tunnel zone must include one or more numbered tunnel interfaces; when the FW/VPN 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:
  - 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 5.0.) 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 & Destination IP.** Configure these options to use VPN Monitoring when the other end of the VPN tunnel is not a NetScreen FW/VPN 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 firewall 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 firewall policy, see “Adding VPN Rules” on page 335.
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 Firewall Policy

Adding XAuth Users

For VPNs that use IPSec manual key to provide remote access services, you must add an XAuth User to the FW/VPN device. An XAuth User has an account on the FW/VPN device that guards the protected resources in the VPN; when the user attempts to connect to a protected resource, the FW/VPN device authenticates the user.

To add a XAuth User for a FW/VPN device, in the FW/VPN 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 FW/VPN 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 Chapter 4, "Configuring Devices".

After you have configured the tunnel zone or interface on the FW/VPN 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.
Chapter 9 Configuring VPNs

Properties

Enter the following values:

- **VPN name.** Enter a name for the VPN.
- **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 FW/VPN 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.

Binding

You can bind the VPN tunnel to a tunnel interface or tunnel zone to increase the number of available interfaces in the FW/VPN 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 & Tunnel Zones” on page 280 and Chapter 4, “Configuring Devices”.

- **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 FW/VPN device to bind the VPN tunnel to the tunnel interface. The FW/VPN device routes all VPN traffic through the tunnel interface to the protected resources.
- **Tunnel Zone.** Select a pre-configured tunnel zone on the FW/VPN device to bind the VPN tunnel directly to the tunnel zone. The tunnel zone must include one or more numbered tunnel interfaces; when the FW/VPN device routes VPN traffic to the tunnel zone, the traffic uses one or more of the tunnel interfaces to reach the protected resources.
**Creating Device-Level VPNs**

**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:
  - 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 5.0.) 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 & Destination IP.** Configure these options to use VPN Monitoring when the other end of the VPN tunnel is not a NetScreen FW/VPN 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 firewall 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 firewall policy, see “Adding VPN Rules” on page 335.
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 Firewall Policy

Adding L2TP Users

For VPNs that use L2TP to provide remote access services, you must add an L2TP User to the FW/VPN device. An L2TP User has an account on the FW/VPN device that guards the protected resources in the VPN; when the user attempts to connect to a protected resource, the FW/VPN device authenticates the user.

To add a L2TP User for a FW/VPN device, in the FW/VPN 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 FW/VPN 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 FW/VPN 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 Chapter 2, “Configuring Role-Based Administration (RBA)”.
  - 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 firewall 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 firewall policy, see “Adding VPN Rules” on page 335.

**Creating L2TP Over Autokey IKE VPNs**

Creating a device-level L2TP-over-Autokey IKE VPN is a six stage process:

1. Add L2TP Users (see “Adding L2TP Users” on page 334)
2. Configure L2TP Settings (see “Configuring L2TP” on page 334)
3. Configure Peer Gateway (see “Configuring Gateways” on page 323)
4. Configure Routes (Route-based only) (see “Configuring Routes (Route-based only)” on page 327)
5. Add VPN to Device (see “Configuring the VPN” on page 328)
6. Add VPN rules to Firewall policy (see “Adding a VPN Rule” on page 335)

**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 FW/VPN policy for each device in the VPN.

Adding a VPN Rule is a three stage process:

1. Configuring the VPN rule
2. Configure firewall policy
3. Installing the firewall policy
Configuring the VPN

In Policy Manager, select a predefined firewall 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 FW/VPN 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 FW/VPN 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 Firewall 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.
- In the **Service** column, select the services you want to permit in the VPN tunnel.

You do not need to configure the action—Security Manager automatically defines the action as tunnel. You can also configure traffic shaping, options, authentication, antivirus, or attack protection for the VPN Rule. For details on configuring these rule options, see Chapter 8, “Configuring Firewall Policies”.

To deny a host, use a deny rule before the VPN rule.

Assign & Install the Firewall Policy

You must assign the firewall policy to each VPN member and install the firewall policy on those devices before the VPN is active.
Section 4: Monitoring
In This Chapter:

- About Realtime Monitor
- Monitoring FW/VPN Devices
- Monitoring VPNs
- Monitoring NSRP Statistics
- Using The Realtime Monitor

The Realtime Monitor module in Security Manager enables you to monitor status and traffic statistics for all the managed FW/VPN 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 FW/VPN devices, VPN tunnels, and NSRP clusters.
ABOUT REALTIME MONITOR

The Realtime Monitor module in Security Manager enables you to monitor real time status and statistics about all the managed FW/VPN 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 FW/VPN 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 FW/VPN devices for security events (failed FW/VPN 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 NetScreen Global PRO, you can continue to use these reports to track Service Level Agreement, traffic, and resource statistics on FW/VPN devices running ScreenOS 4.0.x.

Realtime Monitor Views

Realtime Monitor includes three views:

- **Device Monitor** displays status information on the managed FW/VPN devices in your network. This includes the name and type of each FW/VPN device managed in Security Manager, connection status, and current configuration status. From the Device Monitor, you can also access more detailed information and statistics on each FW/VPN 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 NetScreen security system, you can use the NSRP Monitor to view and troubleshoot the status of FW/VPN devices in clusters within the domain you are working in.
**MONITORING FW/VPN DEVICES**

Use the Device Monitor to get an at-a-glance view of the current status of all the managed FW/VPN devices in your network. Information provided by the Device Monitor includes:

- up/down connection status of the FW/VPN devices
- configuration status of the FW/VPN devices in Security Manager
- name, type and firmware version running on the FW/VPN devices managed in Security Manager

The following table lists and describes all the FW/VPN device information that you can view through the Device Monitor:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name assigned to the FW/VPN device in Security Manager</td>
</tr>
<tr>
<td>Type</td>
<td>Model no. of the FW/VPN device.</td>
</tr>
<tr>
<td>OS Version</td>
<td>ScreenOS firmware version running on the FW/VPN device.</td>
</tr>
</tbody>
</table>
Security Manager retrieves device statistics from the physical FW/VPN device. The device polling interval determines the number of seconds the Device Server waits before polling for new statistics.

### Device Polling Intervals

**Config Status**

Displays the current configuration status of the FW/VPN device in Security Manager as either:

- **“None”** - indicates that no state has been set (does not show in Device Monitor).
- **“Modeled”** - indicates that the FW/VPN device exists in Security Manager but that a connection to the FW/VPN 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 FW/VPN device goes down.
- **“Waiting for 1st connect”** - indicates that Security Manager is waiting for the FW/VPN device to connect. This implies that you must enter a command on the FW/VPN device to make it connect to Security Manager.
- **“Import Needed”** - indicates that you need to import the configuration of the FW/VPN device into Security Manager. When you add a FW/VPN 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 FW/VPN device configuration is still required.
- **“OS Version Adjustment Needed”** - indicates that the firmware version detected running on the device is different than what was previously detected in Security Manager. This could happen in the event that the automatic adjustment option was cleared during a change device firmware directive.
- **“Update Needed”** - indicates that an update to this FW/VPN device is required.
- **“Managed”** - indicates that the FW/VPN device is currently being managed by Security Manager.

**Connection Status**

Displays the connection status of the FW/VPN device in Security Manager as either:

- **“Up”** - FW/VPN device is currently connected to Security Manager.
- **“Down”** - FW/VPN Device is not currently connected to Security Manager, but has connected in the past.
- **“Never Connected”** - FW/VPN device has never connected to Security Manager.

**First Connect**

The first time the FW/VPN device connected to the Security Manager Device Server.

**Latest Connect**

The last time the FW/VPN device connected to the Security Manager Device Server.

**Latest Disconnect**

The last time the FW/VPN device disconnected from the Security Manager Device Server.
You can view the default polling intervals using the Server Manager. Click to select the Device Server and use the Device Polling tab.

You can edit the intervals to meet your monitoring requirements:

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
<th>Poll Interval</th>
<th>Save Interval</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>120</td>
<td>120</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>120</td>
<td>120</td>
</tr>
<tr>
<td>NSRP</td>
<td>Details high availability events and statistics, including VSD group ID, number of units in the cluster, state change counter, init counter, number of Master devices, number of Backup devices, and heartbeat information. Information appears in the NSRP Monitor.</td>
<td>120</td>
<td>120</td>
</tr>
<tr>
<td>Interface</td>
<td>Details the interface number, IP address, and zone to which the interface is mapped. Information appears in the Device Monitor, in the Device Summary.</td>
<td>120</td>
<td>30</td>
</tr>
</tbody>
</table>
Viewing Additional Device Detail and Statistics

If a FW/VPN 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 FW/VPN 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 FW/VPN device that is up and running by viewing the Device Detail Status. To view the Device Detail Status on a particular FW/VPN device, right-click on the FW/VPN device and select **View Details** or simply double-click the FW/VPN device.

<table>
<thead>
<tr>
<th>Device Detail Status</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>OS Version</td>
<td>5.0.0</td>
</tr>
<tr>
<td>Mode</td>
<td>Route/Transparent/Network Address Translation (NAT)</td>
</tr>
<tr>
<td>Latest Reboot</td>
<td>Mon Apr 08 00:37:35 PDT 2002</td>
</tr>
<tr>
<td>CPU Utilization</td>
<td>2%</td>
</tr>
<tr>
<td>1 Min Load</td>
<td>4%</td>
</tr>
<tr>
<td>5 Min Load</td>
<td>3%</td>
</tr>
<tr>
<td>15 Min Load</td>
<td>3%</td>
</tr>
<tr>
<td>Mem Allocated</td>
<td>446 MB</td>
</tr>
<tr>
<td>Mem Left</td>
<td>494 MB</td>
</tr>
<tr>
<td>Mem Fragmented</td>
<td>8 KB</td>
</tr>
<tr>
<td>Active Sessions</td>
<td>1</td>
</tr>
<tr>
<td>Allocated Sessions</td>
<td>1</td>
</tr>
<tr>
<td>Max Sessions</td>
<td>1000000</td>
</tr>
<tr>
<td>Failed Sessions</td>
<td>0</td>
</tr>
</tbody>
</table>
The following table lists and describes all the information that you can view through the Device Detail Status:

<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 FW/VPN device.</td>
</tr>
<tr>
<td>Mode</td>
<td>Current operation mode of the FW/VPN 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 FW/VPN device was powered off and on. You can use this information to determine how long the FW/VPN 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 FW/VPN device for the last 1 min.</td>
</tr>
<tr>
<td>5 Min. Load</td>
<td>The percent CPU utilization average on the FW/VPN device for the last 5 mins.</td>
</tr>
<tr>
<td>15 Min. Load</td>
<td>The percent CPU utilization average on the FW/VPN device for the last 15 mins.</td>
</tr>
<tr>
<td>Mem Allocated</td>
<td>The original amount of memory allocated to the FW/VPN device.</td>
</tr>
<tr>
<td>Mem Left</td>
<td>The amount of allocated memory that remains after being used by the FW/VPN device.</td>
</tr>
<tr>
<td>Mem Fragmented</td>
<td>The amount of fragmented memory.</td>
</tr>
<tr>
<td>Active Sessions</td>
<td>The number of active sessions on the FW/VPN device.</td>
</tr>
<tr>
<td>Allocated Sessions</td>
<td>The number of sessions originally allocated to the FW/VPN device.</td>
</tr>
<tr>
<td>Max Sessions</td>
<td>The maximum number of sessions on the FW/VPN device.</td>
</tr>
<tr>
<td>Failed Sessions</td>
<td>The number of sessions that have failed on the FW/VPN device.</td>
</tr>
</tbody>
</table>

**Viewing Device Statistics**

If a FW/VPN 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 FW/VPN device, right-click on the FW/VPN 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 FW/VPN device or virtual system, for example, serial number and IP address, type, and firmware version.
- Interface information
- Device status
- Time-related statistics (i.e., last connect, reboot, etc.)
The following table lists and describes all the information that you can view about a particular FW/VPN device from the Device Statistics Summary.

<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 FW/VPN device. Vsys: Displays the serial number of the FW/VPN device.</td>
</tr>
<tr>
<td>Vsys</td>
<td>The name of the virtual system (if applicable)</td>
</tr>
<tr>
<td>Version</td>
<td>The FW/VPN 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 Data Collector the FW/VPN 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 FW/VPN device (this is not displayed in the Vsys view).</td>
</tr>
<tr>
<td>Last Known Connect Time</td>
<td>The last time the FW/VPN device connected to the Data Collector (this is not displayed in the Vsys view).</td>
</tr>
<tr>
<td>Device Status</td>
<td>Whether the FW/VPN 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 FW/VPN device is down, the entry lists the last time it was up. Used to determine how long a FW/VPN device was down (this is not displayed in the Vsys view).</td>
</tr>
<tr>
<td>GMT Time Offset (Hours)</td>
<td>The hour the FW/VPN 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 FW/VPN 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 FW/VPN device. You can also use Troubleshooting to access the send “get commands” window in order to further diagnose and troubleshoot potential issues.

The following table describes each device-specific view.

<table>
<thead>
<tr>
<th>View Type</th>
<th>View</th>
<th>Allows you to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic</td>
<td>Policy Distribution</td>
<td>View traffic on the FW/VPN device distributed by policy. Allows 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 FW/VPN device distributed by protocol. Allows 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 FW/VPN device (if applicable). Also allows you to view a chart of the VPN distribution by VPN tunnel.</td>
</tr>
<tr>
<td>Interface</td>
<td>Ethernet Statistics</td>
<td>View FW/VPN device traffic over specific interfaces. Allows you to view a chart of the utilization distributed by interface.</td>
</tr>
<tr>
<td></td>
<td>Flow Statistics</td>
<td>View FW/VPN device traffic on flow counters over specific interfaces. Allows you to view a chart of flow statistics distributed by interface.</td>
</tr>
<tr>
<td></td>
<td>Attack Statistics</td>
<td>View all of the attacks that have occurred on a FW/VPN device over specific interfaces. Allows you to view a chart of attacks distributed by interface.</td>
</tr>
<tr>
<td>Zone</td>
<td>Ethernet Statistics</td>
<td>View FW/VPN device traffic from specific zones. Allows you to view a chart of the traffic distributed by zone.</td>
</tr>
<tr>
<td></td>
<td>Flow Statistics</td>
<td>View FW/VPN device traffic on flow related statistics for specific interfaces. Allows you to view a chart of flow statistics distributed by zone.</td>
</tr>
<tr>
<td></td>
<td>Attack Statistics</td>
<td>View all counters related to attacks that have occurred on a FW/VPN device from specific zones. Allows you to view a chart of the attacks distributed by zone.</td>
</tr>
<tr>
<td>System</td>
<td>Resource Statistics</td>
<td>View CPU utilization and memory allocation statistics on the FW/VPN device. Allows you to view CPU, Memory and Session Utilization trends.</td>
</tr>
<tr>
<td></td>
<td>Active Statistics</td>
<td>View administrator and user activities; active VPNs; and authenticated users on a FW/VPN device. Also allows you to view a snapshot of the ongoing active sessions on the FW/VPN device.</td>
</tr>
<tr>
<td></td>
<td>Troubleshooting</td>
<td>Send troubleshooting commands over Telnet or SCS to a specific FW/VPN device.</td>
</tr>
<tr>
<td>HA</td>
<td>NSRP Statistics</td>
<td>View NSRP statistics related to clusters created on the FW/VPN device (if applicable).</td>
</tr>
</tbody>
</table>
Viewing Device Traffic Distribution

You can view statistics describing the traffic on a specific FW/VPN device including how the traffic is distributed (i.e., either 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 FW/VPN device.

Viewing Traffic Distribution by Policy

Click on the Policy Distribution node to view FW/VPN device traffic that matches the access policies configured for a FW/VPN 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.

The following table describes all of the information that is available from the Policy Distribution view..

<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>
</tbody>
</table>
Monitoring FW/VPN Devices

You can adjust all elements depicted in the graph including the policies, data values (i.e., 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.

**Viewing Traffic Distribution by Protocol**

Click on 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 FW/VPN 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.
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 FW/VPN device.</td>
</tr>
<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 FW/VPN 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 FW/VPN 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 FW/VPN 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 FW/VPN 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>

**Adjusting Data Depicted Graphically**

You can adjust the interfaces (i.e., Trust, Untrust, Management, NSRP, and Self) and data depicted graphically in the same way that you adjust the Policy Distribution graphs.

**Note:** Additional options allow you to adjust the data types in the Protocol Distribution graph by Bytes In, Bytes Out, Packets In, Packets Out, or Utilization, and by Interface.
Viewing Traffic Distribution by VPN (if applicable)

If you are using your FW/VPN devices to implement VPNs, you can view how traffic is being distributed across each different VPN tunnel on the FW/VPN 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 (i.e., absolute or delta), and type of data (bytes in or out, packets in or out, utilization).

Adjusting VPN Tunnels Depicted Graphically:

1. Right-click on 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 on the Chart view and select Data, and either Delta or Absolute.
2. Right-click on 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 on 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 (i.e., name, Policy ID, group and user associations, VPN type)
- Security Association (SA) information
- total number of data over the tunnel (i.e., bytes in/out, packets in/out, utilization)

The following table describes all of the information that is available from the 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>
<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 FW/VPN 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>
</tbody>
</table>
Click on 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 (i.e., name, Policy IP, local and peer gateway IDs and IP addresses)
- Security established on the active VPN
- Time-related statistics (i.e., 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>Name</td>
<td>The name of the active VPN.</td>
</tr>
<tr>
<td>VPN Type</td>
<td>Type of tunnel: Site-to-site or dial-up.</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>Whether the tunnel for the active VPN is UP or Down.</td>
</tr>
<tr>
<td>Ave Latency</td>
<td>A rolling average of latency, presented in milliseconds.</td>
</tr>
<tr>
<td>Last Latency</td>
<td>Latency for the last ping response.</td>
</tr>
<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>
</tbody>
</table>

### Viewing Active VPN Information

Click on 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 (i.e., name, Policy IP, local and peer gateway IDs and IP addresses)
- Security established on the active VPN
- Time-related statistics (i.e., 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>Name</td>
<td>The name of the active VPN.</td>
</tr>
<tr>
<td>VPN Type</td>
<td>Type of tunnel: Site-to-site or dial-up.</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>Whether the tunnel for the active VPN is UP or Down.</td>
</tr>
<tr>
<td>Ave Latency</td>
<td>A rolling average of latency, presented in milliseconds.</td>
</tr>
<tr>
<td>Last Latency</td>
<td>Latency for the last ping response.</td>
</tr>
<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>
</tbody>
</table>
Monitoring FW/VPN Devices

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 FW/VPN device. Depending upon the specific FW/VPN device, the following interfaces will apply:

- Trust and Untrust interfaces available on all FW/VPN devices.
- DMZ interface available on NetScreen-25, NetScreen-50, NetScreen-100 and NetScreen-500 devices; the NetScreen-5XP device has no DMZ interface.
Chapter 10 Monitoring

- HA interface and management interface available on NetScreen-100 and NetScreen-500 devices.

Ethernet Statistics apply only to FW/VPN devices, and not to virtual systems.

A graph appears displaying FW/VPN device % utilization traffic on the interface. Right-click within the chart to select a desired Interface (i.e., 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>
<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 FW/VPN 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 FW/VPN device.</td>
</tr>
</tbody>
</table>
Monitoring FW/VPN Devices

Item | Displays...
--- | ---
Delta Bytes Out | the total numerical difference between the current bytes out value and the previous bytes out value.
Packets In | the number of incoming packets handled by the interface through the FW/VPN device.
Delta Packets In | the total numerical difference between the current packets in value and the previous packets in value.
Packets Out | the number of outgoing packets handled by the interface through the FW/VPN device.
Delta Packets Out | the total numerical difference between the current packets out value and the previous packets out value.
Broadcast | the number of broadcast-type packets processed through the FW/VPN device over the selected interface.
CRC Errors | the number of packets generating a cyclic redundancy code error processed through the FW/VPN device over the selected interface.
Alignment Errors | the number of Frame Checksum (FCS) errors.
ShortFrame | the number of frames that are not of the correct length.
RXCollision | the number of times that two packets collide, resulting in damage to both. This indicates that the network is overloaded.
Speed (Mbps) | This is useful in calculating the speed of the interface.
Status | whether the FW/VPN device is currently Up or Down.
Direction | whether the FW/VPN device is in half or full duplex mode.
Zone | the name of the zone associated with the interface.

**Viewing Flow Statistics**

Click on the **Flow Statistics** node to view data for various flow counters on a specific FW/VPN device or virtual interface. For each FW/VPN 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>
<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 FW/VPN device over the selected interface.</td>
</tr>
<tr>
<td>Bytes Out</td>
<td>the number of bytes of outgoing traffic processed through the FW/VPN device over the selected interface.</td>
</tr>
<tr>
<td>Packets In</td>
<td>the number of incoming packets processed through the FW/VPN device over the selected interface.</td>
</tr>
<tr>
<td>Packets Out</td>
<td>the number of outgoing packets processed through the FW/VPN device over the selected interface.</td>
</tr>
<tr>
<td>VLAN In</td>
<td>the number of VLAN packets received through the NetScreen FW/VPN device; applies to virtual systems.</td>
</tr>
<tr>
<td>VLAN Out</td>
<td>the number of VLAN packets sent through the NetScreen FW/VPN 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>
</tbody>
</table>
Click on the **Attack Statistics** node to view distribution of the attacks that have occurred on a specific FW/VPN 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>
<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>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 FW/VPN 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 FW/VPN device to detect and reject oversized or irregular packet sizes.</td>
</tr>
<tr>
<td>Address Spoofing</td>
<td>You can enable a FW/VPN 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 FW/VPN 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. FW/VPN 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 FW/VPN device ignores further UDP packets for the remainder of that second.</td>
</tr>
<tr>
<td>WinNuke</td>
<td>WinNuke can cause any computer on the Internet running Windows to crash. WinNuke introduces a NetBIOS anomaly that forces Windows to restart. FW/VPN devices can scan any incoming Microsoft NetBIOS Session Service packets, modify them, and record the event as a WinNuke attack.</td>
</tr>
<tr>
<td>Item</td>
<td>Displays</td>
</tr>
<tr>
<td>------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</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 FW/VPN device internally logs the number of different ports scanned from one remote source. If a remote host scans 10 ports in 0.3 seconds, NetScreen 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 FW/VPN 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>
<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 FW/VPN 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 FW/VPN 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 FW/VPN 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 FW/VPN 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 FW/VPN 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>
</tbody>
</table>
### Chapter 10 Monitoring

<table>
<thead>
<tr>
<th>Item</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Strict Src</td>
<td>The FW/VPN 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 FW/VPN 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 FW/VPN 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 FW/VPN device monitors each HTTP packet and detects any URL that matches any of several user-defined patterns. The FW/VPN device automatically drops any such packet.</td>
</tr>
<tr>
<td>Limit Session</td>
<td>FW/VPN devices can limit the number of sessions that can be established by a single IP address. For example, session resources on a Web server can be exhausted if there are many requests from the same client. This option defines the maximum number of sessions the FW/VPN device can establish per second for a single IP address. (The default threshold is 128 sessions per second per IP address.)</td>
</tr>
<tr>
<td>Block Frag</td>
<td>As packets traverse different networks, it is sometimes necessary to break a packet into smaller pieces (fragments) based upon the network’s maximum transmission unit (MTU). IP fragments may carry an attacker’s attempt to exploit the vulnerabilities in the packet reassembly code of specific IP stack implementations. When the target system receives these packets, the results range from not processing the packets correctly to crashing the entire system. When you enable the FW/VPN device to deny IP fragments on a security zone, the FW/VPN device blocks all IP packet fragments that it receives at interfaces bound to that zone.</td>
</tr>
<tr>
<td>Zone</td>
<td>the name of the zone associated with the attack.</td>
</tr>
</tbody>
</table>
Viewing Zone Statistics

You can also view traffic information as it is processed by a FW/VPN 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 FW/VPN device.

Viewing Resource Statistics

Click on the Resource Statistics node to view the resources for a FW/VPN device. The following table describes all of the information that is available from the Resource Statistics view:

<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 FW/VPN device.</td>
</tr>
<tr>
<td>Memory Allocated</td>
<td>the current memory allocation to FW/VPN 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>
</tbody>
</table>
Chapter 10 Monitoring

Click on the Active Statistics node to view administrator and user activities for a FW/VPN 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>
<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>
<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 FW/VPN device. You can view active sessions from the *Active Statistics* view.

When you click on the Active Sessions tab, a short form view of the active sessions appears enabling you to monitor basic information (i.e., 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 FW/VPN device by default. You can also view extended information about the session (i.e., 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>
<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>
<tr>
<td>Source Port</td>
<td>Port number of the sending node of the connection.</td>
</tr>
<tr>
<td>Destination IP</td>
<td>IP address of the receiving node of the connection.</td>
</tr>
<tr>
<td>Destination Port</td>
<td>Port number of the receiving node of the connection.</td>
</tr>
<tr>
<td>Translated IP</td>
<td>Translated IP address.</td>
</tr>
<tr>
<td>Translated Port</td>
<td>Translated port number.</td>
</tr>
<tr>
<td>Duration (sec)</td>
<td>Length in seconds of the connection session.</td>
</tr>
<tr>
<td>Policy ID</td>
<td>A unique identifier specified when the policy was configured. None means no name was specified during policy configuration.</td>
</tr>
<tr>
<td>Protocol ID</td>
<td>A unique identifier specified when the protocol was configured.</td>
</tr>
<tr>
<td>ICMP Type</td>
<td>the type of ICMP protocol.</td>
</tr>
<tr>
<td>Bytes In</td>
<td>the total number of bytes sent in.</td>
</tr>
<tr>
<td>Bytes Out</td>
<td>the total number of bytes sent out.</td>
</tr>
<tr>
<td>Total Packets</td>
<td>the total number of packets sent.</td>
</tr>
<tr>
<td>Duration</td>
<td>the length in seconds of the connection session.</td>
</tr>
<tr>
<td>Start Time</td>
<td>the time that the session started.</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. The Session Filter allows you to fetch specific sessions on a FW/VPN 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. Once 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**

You can also communicate using Telnet or a Secure Command Shell to query on the status of a FW/VPN device. You can use this capability to issue a “get” Telnet command to a FW/VPN device or a NetScreen CLI command to the SCS (Secure Command Shell) on the FW/VPN device to troubleshoot problems.
Viewing High Availability (HA) Statistics (if applicable)

If you have configured FW/VPN 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>
<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 FW/VPN 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</td>
</tr>
<tr>
<td></td>
<td>process of joining the VSD (or RTO) group.</td>
</tr>
<tr>
<td>Master</td>
<td>the number of Master FW/VPN devices.</td>
</tr>
<tr>
<td>Primary BackUp</td>
<td>the number of primary backup FW/VPN devices.</td>
</tr>
<tr>
<td>BackUp</td>
<td>the total number of backup FW/VPN devices.</td>
</tr>
<tr>
<td>Ineligible</td>
<td>Notes that an administrator purposefully assigned a FW/VPN device so</td>
</tr>
<tr>
<td></td>
<td>that it cannot participate in the selecting a new master FW/VPN device.</td>
</tr>
<tr>
<td>InOperable</td>
<td>Notes that a VSD (or RTO) group FW/VPN device has an internal problem.</td>
</tr>
<tr>
<td>Master Conflict</td>
<td>the number of conflicts that occurred on the master FW/VPN device.</td>
</tr>
<tr>
<td>Primary Backup Conflict</td>
<td>the number of conflicts that occurred on the primary backups FW/VPN</td>
</tr>
<tr>
<td></td>
<td>device.</td>
</tr>
<tr>
<td>Tx Heartbeat</td>
<td>the number of transmitted heartbeats on the FW/VPN devices.</td>
</tr>
<tr>
<td>Rx Heartbeat</td>
<td>the number of received heartbeats on the FW/VPN devices.</td>
</tr>
</tbody>
</table>
**MONITORING VPNs**

If you have implemented a virtual private network or VPN, you can use the VPN Monitor to get an at-a-glance status of the up/down status of every VPN tunnel as well as other statistics relevant to your VPN.

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>
<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 FW/VPN devices used in the VPN. For example, a root FW/VPN 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 Hostname(IP)(Vsys)</td>
<td>Destination FW/VPN devices used in the VPN. For example, a root FW/VPN 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>Status</td>
<td>VPN Status: Up or Down</td>
</tr>
</tbody>
</table>

**Note:** You must enable the “VPN Monitor” option on the tunnel when configuring the tunnel for the device.
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 FW/VPN device or virtual system associated with the VPN tunnel that you want to view. Click on the **Refresh** button to apply the Session Display criteria to the active session table view.

**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 FW/VPN device or virtual system associated with the VPN tunnel that you want to view. Click on 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 on the VPN tunnel and select **Active VPN Details**).

Refer to “**Viewing Active VPN Information**” on page 354 for more information on the Active VPN Details table.

**Viewing Device-Specific VPN Information**

Right-click on the VPN tunnel and select **Monitor Data**, and then the FW/VPN device to view FW/VPN 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 FW/VPN device.

<table>
<thead>
<tr>
<th>SPI (in/out)</th>
<th>Security Parameter Index (SPI) key into and out of the active VPN. This is the encryption method.</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP (Local-Peer)</td>
<td>Peer gateway IP address for the active VPN.</td>
</tr>
<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>
**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 NetScreen systems that are in “clusters.” These systems include both the NetScreen-500 and the NetScreen-1000. To launch the NSRP Monitor, click on the **NSRP Monitor** node.

Double-click on 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 (i.e., 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>Item</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster</td>
<td>name of this cluster.</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>
</tbody>
</table>
Double-click on the cluster FW/VPN device icon or click on the + icon that corresponds to the cluster FW/VPN device icon to view the virtual security devices (VSD) and run-time objects (RTO) that have been attached to this cluster.

Click on 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>
<thead>
<tr>
<th>Item</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<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>
</tbody>
</table>

**Viewing VSD/RTO Information**

Double-click on the cluster FW/VPN device icon or click on the + icon that corresponds to the cluster FW/VPN device icon to view the virtual security devices (VSD) and run-time objects (RTO) that have been attached to this cluster.

Click on 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>
<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 FW/VPN 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 FW/VPN device.</td>
</tr>
<tr>
<td>Master</td>
<td>the Master NetScreen System.</td>
</tr>
<tr>
<td>Primary Backup</td>
<td>the primary NetScreen 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>
<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>
<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>
Chapter 10 Monitoring

USING THE REALTIME MONITOR

The following examples describe typical use cases for monitoring your FW/VPN devices, VPNs, and NSRP clusters in 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 FW/VPN devices managed in your network. You are using Security Manager to manage your network, and Realtime Monitor to monitor the up/down connection status of all your FW/VPN devices.

One day, you notice that the Connection Status on a mission-critical FW/VPN device indicates that the FW/VPN device is DOWN. You wait several minutes to verify that the connection status doesn’t resolve itself as intermittent network problems may cause a FW/VPN device to temporarily indicate as DOWN. The Device Monitor still indicates that the FW/VPN device is DOWN.

You next try to ping the FW/VPN device. If you are successful in reaching the device, you can send a `get status` command to check the status of the FW/VPN device.

If you cannot ping the FW/VPN device, you will want to investigate further what may be a potential problem with the FW/VPN device or your network. You next scan the Log Viewer for the log entry indicating that the FW/VPN device has disconnected. You can filter the log entries in the Log Viewer to display only the log entries generated for the FW/VPN 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 FW/VPN device disconnecting. This will help you to determine the cause of the problem.

You notice several very suspicious log entries that indicate that this FW/VPN 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.
In This Chapter:

- About Logging
- Managing Log Volume
- Configuring Logging
- Using the Log Viewer
- Using the Log Investigator
- Using the Audit Log Viewer

Security Manager’s highly integrated log environment enables you to easily distill information. Much of the same data presented as descriptive column information in a logging environment is easily accessible in the reporting environment. This linkage enables you to interpret event information in a specific context. However, if you desire, you can have more information available simply by staying in the logging environment. Security Manager links location information with port detail enabling you to determine attack types based on suspicious overuse of various ports.

Security Manager integrates two areas of the logging environment that provide varying levels of detail. One environment, the Log Viewer, provides all details while the other, the Log Investigator, enables you to view cross-tabulations between sources, destinations, attacks and destination ports.
About Logging

Security Manager logging tools provide a high-level view of activity over your distributed firewall environment. Typically, you accumulate log entries across domains from multiple devices. The logging tools in Security Manager help identify patterns that enable you to isolate specific devices in a large collection of devices on an enterprise network that are the source of certain problems you tracked.

You can control the amount of information displayed in the logging environments. You can view events across all domains, device groups, clusters, and firewalls and see the results of the event in all parts of your network.

The Security Manager logging environment provides centralized control and tracking enabling you more access to details over all of your distributed firewall network. It provides centralized access to logging data through a central console. From the central console, you can control logging behavior by adding rules.

It provides a view from a centralized administrator console enabling you to view events at desired local positions across the enterprise. With one central database, you can easily publish data on your intranet to each business unit with built-in reporting. Reports can separate by domains. Note that you cannot save Log Investigator views to a file or print them. The logging tools in Security Manager enable you to enforce policies by tracking what packets generated denials and other traffic related messages.

About Logs

A log is a record of an event that occurred on a NetScreen FW/VPN device. Devices generate log entries when:

- An event matches a firewall rule in which logging is enabled. When a rule has logging configured as an action, the device creates a log for events that match that rule.
- An event matches a predefined set of conditions configured on a managed device or the management server.

Logs appear in the Log Viewer in the order they are received. You can use the Log Viewer to analyze log entries and determine the effectiveness of your current firewall policies and device configurations.

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.
Log Categories

Security Manager supports the following log entry categories:

<table>
<thead>
<tr>
<th>Log Type</th>
<th>Generated When</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm</td>
<td>When Security Manager detects a violation of a firewall rule with an alarm threshold.</td>
</tr>
<tr>
<td>Anomaly</td>
<td>When Security Manager detects an event that matches a protocol anomaly attack group.</td>
</tr>
<tr>
<td>Config</td>
<td>When a configuration or operational state changed in Security Manager.</td>
</tr>
<tr>
<td>Custom</td>
<td>When Security Manager detects an event that matches a custom signature.</td>
</tr>
<tr>
<td>Info</td>
<td>Details general system information.</td>
</tr>
<tr>
<td>Self</td>
<td>When Security Manager detects an event that is non-traffic related.</td>
</tr>
<tr>
<td>Signature</td>
<td>When Security Manager detects an event that matches a known attack pattern.</td>
</tr>
<tr>
<td>Traffic</td>
<td>When Security Manager detects a traffic-based detection violation.</td>
</tr>
<tr>
<td>Screen</td>
<td>When Security Manager detects a NetScreen Screen-level attack.</td>
</tr>
<tr>
<td>Implicit</td>
<td>Contains implicit attack signatures.</td>
</tr>
</tbody>
</table>

Log Severity Levels

The log severity level defines the degree to which the log is considered to be urgent to the network administrator. All log entries have a predefined severity level assigned to them in the NetScreen FW/VPN device firmware. The severity level assigned to each log depends on the log category or type of log being generated, for example, information, traffic, or configuration log entries. The following table describes the severity levels.

<table>
<thead>
<tr>
<th>Severity Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>No severity level specified.</td>
</tr>
<tr>
<td>Emergency</td>
<td>The most urgent level of severity.</td>
</tr>
<tr>
<td>Alert</td>
<td>The second most urgent level of severity.</td>
</tr>
<tr>
<td>Critical</td>
<td>A noteworthy level of severity.</td>
</tr>
<tr>
<td>Error</td>
<td>A severity level that indicates an error occurred.</td>
</tr>
<tr>
<td>Warning</td>
<td>A severity level that indicates no error or violation, but is a cautioning that questionable activity may have occurred.</td>
</tr>
<tr>
<td>Notification</td>
<td>The least urgent severity level.</td>
</tr>
<tr>
<td>Information</td>
<td>A non-severity text message describing an event.</td>
</tr>
<tr>
<td>Debugging</td>
<td>Debugging text.</td>
</tr>
</tbody>
</table>
You can configure a NetScreen FW/VPN device to log only those events that meet a specific severity level criteria. You can also configure the device to forward log entries that contain a specific severity to a specific destination, such as a console location, internal, or syslog server. Also note that you can specify log entries with different severity levels to be forwarded to the same log destination.

**About Log Modules**

To see what events occur on your network, view the log entries using the following three Security Manager modules:

- **Log Viewer** to view complete, summarized, or detailed log entry information. The Log Viewer enables you to view an individual log entry and analyze raw data (either all, or only a subset using filters). It allows you to find specific information. The Log Viewer displays log entries in table format. You control the data selected by using filters or column settings.

- **Log Investigator** to correlate log data. The Log Investigator is an exploratory data analysis tool that crosstabulates on two dimensions and hyperlinks from the Report Manager to the Log Viewer. The Log Investigator lets you provide interactive analysis of summary data.

- **Audit Log Viewer** to detect a change on your firewall device through Security Manager, who performed the change, and what time the change occurred. Also, you can view job results.

From these modules, you can quickly navigate to the policy and make necessary changes.

**About Log Volumes**

Security administrators have different requirements with respect to how many log entries are useful. Some want large numbers of log entries, even though they may not have time to review all the data immediately. Some want only more manageable numbers of log entries that they can view within a short period.

To gather information quickly from large numbers of log entries, view summary information in the following Security Manager modules:

- For details on using the Log Viewer to manage log entries, see “Managing Logs” on page 401.

- For details on using the Log Investigator, see “Using the Log Investigator” on page 418.

- For details on using the Report Manager, see Chapter 12, “Reporting”.

For details on archiving, retrieving, and purging log entries from the management system, see “Managing Log Volume” on page 380.
Understanding Log Flow

Before beginning to learn about various aspects of the NetScreen Security Manager logging environment, you may find it helpful to first understand how log entries flow to and from various entities in the environment.

A NetScreen FW/VPN device generates a log when the event matches the logging conditions. For example, when an administrator logs onto a NetScreen FW/VPN device, the device generates an information log which records details of that event. As you will see in the next few sections, NetScreen pre-configured devices to a number of different types of log entries. After the device generates the log, the data is stored as a log database within the Device Server. It remains in the log database. A logging tool then displays the contents of a number of fields contained by the log.

After the log entries are in the Log Database, the administrator can use two logging tools to access them. The Log Viewer obtains each log as it comes into the database, taking each one in real-time and displaying its fields in the Log Viewer. The Log Investigator fetches data upon user request.

It may be helpful for you to visualize log entries being sent or pushed from the device to the Device Server which in turn pushes the log entries to the Log Database. After log entries are in the Log Database, they are requested or pulled from the two logging tools. Then the view of the log entries becomes available on your network management console where you can view them through the tools.

The following diagram characterizes the flow of log entries in the NetScreen environment from the NetScreen FW/VPN device to the console.
Managing Log Volume

While logging provides many benefits in terms of making information available, it also creates traffic on your network. Because this traffic can interfere with performance, you should balance log generation with the performance needs of your system. Be aware of the Expected Log Rates (ELRs) associated with devices. The Security Manager management server can process up to 20,000 log entries per second.

The following table details some common logging capacity values. Review it to better assess your logging environment needs. Be aware that most of the capacity figures are very large and probably exist only in theory. You need to obtain a sense of your device's individual limit within the context of the maximum values. The most secure figure to rely on is the Receivable Rate Per Second figure, also provided.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Maximum Value for Any Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall Memory Capacity Per-Day in Security Manager</td>
<td>256 Gbytes of log entries per day. (appr.)</td>
</tr>
<tr>
<td>Overall Log Capacity Per-Day in Security Manager</td>
<td>2 billion log entries per day. (appr.)</td>
</tr>
<tr>
<td>Receivable Rate Per Second (Device Server)</td>
<td>20,000 log entries per second</td>
</tr>
<tr>
<td>Receivable Rate Per Day</td>
<td>1.7 billion log entries per day</td>
</tr>
</tbody>
</table>

The receivable rates per second for each NetScreen FW/VPN device are shown below:

<table>
<thead>
<tr>
<th>Device</th>
<th>Number of Logs</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetScreen-100</td>
<td>14,300</td>
</tr>
<tr>
<td>NetScreen-500</td>
<td>14,300</td>
</tr>
<tr>
<td>NetScreen-50</td>
<td>1,000</td>
</tr>
<tr>
<td>NetScreen-204</td>
<td>500</td>
</tr>
<tr>
<td>NetScreen-208</td>
<td>500</td>
</tr>
<tr>
<td>NetScreen-25</td>
<td>1,000</td>
</tr>
<tr>
<td>NetScreen-5XT</td>
<td>14,300</td>
</tr>
<tr>
<td>NetScreen-5XP</td>
<td>14,300</td>
</tr>
<tr>
<td>NetScreen-5200</td>
<td>24,500</td>
</tr>
<tr>
<td>NetScreen-5400</td>
<td>24,500</td>
</tr>
</tbody>
</table>

**Note:** The Log Viewer and the Log Investigator receive log entries in different fashions, influencing how many log entries you will see in an early view of each tool. The Log Viewer obtains log entries one by one while the Log Investigator obtains collections of log entries at one time.
Archiving Logs

You can archive and retrieve log entries to and from a storage device using standard Unix commands. Logs reside on the GUI Server, so you need to transfer them from the GUI Server to the storage device.

Before you begin archiving, you must stop the processes running on the GUI Server. If you are archiving the current day's logs, you must also stop processes running on the Device Server. After you have completed archiving, restart the processes. For details on stopping, starting, and restarting processes on the management system, see the NetScreen-Security Manager Installer's Guide.

To archive, run the appropriate command on your Solaris or Linux platform on all data and files in two paths:

- For all information located on the GUI Server: /usr/netscreen/GuiSvr/var
- For all information located on the Device Server: /usr/netscreen/DevSvr/var

Recommended commands to use in these paths are:
- the `tar` command
- the `scp` (Secure Copy) command
- the `ftp` (File Transfer Protocol) command

For full descriptions and options for each command, see appropriate documentation or man pages.

Purging Logs

To change the threshold for log entries to be purged, you need to change a threshold value in the Security Manager configuration file. You access this file through the following path:

```
\usr\netscreen\devsvr\var
```

You can change the Storage Manager.threshold field value which contains the upper limit for the number of log entries that can be stored on the Log Server. The default is 100. You can also change the amount of free space allowed in Kbytes by changing the Storage Manager.MnalFreespace value. The default is 200.

Exporting Logs

You can also export log entries for use in other applications. For details on configuring the GUI Server to automatically export log entries, see “Configuring the GUI Server for Logging” on page 394.
Chapter 11 Logging

**Configuring Logging**

Before you can receive log entries, you must configure logging. You can configure the following types of logging:

- **Configuring Device-Level Logging.** Configure logging for an individual NetScreen FW/VPN device configuration.
- **Configuring Logging in Firewall Rules.** Configure logging for multiple devices in a firewall rule.
- **Configuring the GUI Server for Logging.** Set log criteria and configure log actions (export, email, etc.) for all managed devices in the GUI Server settings.

Some log types are always enabled, such as configuration log entries and information log entries. For details on these log types, see “Other Log Types” on page 395.

**About Log Types**

NetScreen FW/VPN devices generate log entries based on events. The following table describes the three basic event types.

<table>
<thead>
<tr>
<th>Column</th>
<th>What it means</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Events</td>
<td>An event occurred that matched a firewall rule. A log entry was created to record the event and sent to Security Manager.</td>
</tr>
<tr>
<td>Alarm Events</td>
<td>An event occurred that violated an alarm for a type of network activity. A log entry was created to record the event and sent to Security Manager.</td>
</tr>
<tr>
<td>Statistics</td>
<td>An event that reports which activity has occurred during a given timeframe and what or who caused the activity.</td>
</tr>
</tbody>
</table>

Some event types generate log entries that appear in the Log Viewer, while others appear in RealTime Monitor.

The following table details the location of event-generated log entries:

<table>
<thead>
<tr>
<th>Category</th>
<th>Events Supported</th>
<th>Destination</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarms</td>
<td>Attack, Traffic, Other</td>
<td>Log Viewer</td>
<td>Displays all events that violated a set threshold.</td>
</tr>
<tr>
<td>VPN</td>
<td>VPN Events</td>
<td>Realtime Monitor &gt; VPN Monitor</td>
<td>Displays events related to the VPN tunnel.</td>
</tr>
</tbody>
</table>
Configuring Logging

You configure different areas of Security Manager to set conditions to generate each log type, as shown below:

<table>
<thead>
<tr>
<th>Log Type</th>
<th>Where Configured</th>
<th>Where Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm</td>
<td>Device Configuration &gt; Report Settings &gt; NSM Policy Manager &gt; Rule Options &gt; Log/Count</td>
<td>In device configuration In firewall rule</td>
</tr>
<tr>
<td>Anomaly</td>
<td>Policy Manager &gt; Rule Options &gt; Attack Protection</td>
<td>In firewall rule</td>
</tr>
<tr>
<td>Config N/A</td>
<td>Always enabled</td>
<td></td>
</tr>
<tr>
<td>Custom</td>
<td>Policy Manager &gt; Rule Options &gt; Attack Protection</td>
<td>In firewall rule</td>
</tr>
<tr>
<td>Info</td>
<td>Configured by default</td>
<td>Always enabled</td>
</tr>
<tr>
<td>Self</td>
<td>Device Configuration &gt; Report Settings &gt; General</td>
<td>In device configuration</td>
</tr>
<tr>
<td>Signature</td>
<td>Device Configuration &gt; Report Settings &gt; NSM Policy Manager &gt; Rule Options &gt; Attack Protection</td>
<td>In firewall rule In device configuration</td>
</tr>
<tr>
<td>Traffic</td>
<td>Device Configuration &gt; Report Settings &gt; NSM Policy Manager &gt; Rule Options &gt; Log/Count</td>
<td>In device configuration In firewall rule</td>
</tr>
<tr>
<td>Screen</td>
<td>Device Configuration &gt; Network &gt; Zone</td>
<td>In device configuration</td>
</tr>
<tr>
<td>Implicit</td>
<td>N/A</td>
<td>Always enabled</td>
</tr>
</tbody>
</table>

The following sections detail how to configure your managed devices to generate each supported log type.

**Configuring Device-Level Logging**

The following sections detail how to configuring logging at the individual device-level.
Configuring SCREEN Logs

Screen attack log entries enable you to set thresholds for designated SCREEN attacks. To secure all connection attempts, NetScreen FW/VPN devices use a dynamic packet filtering method known as stateful inspection. Using this method, the NetScreen FW/VPN device notes various components in a TCP packet header. This includes source and destination IP addresses, source and destination port numbers, and packet sequence numbers. The device maintains the state of each TCP session traversing the firewall.

NetScreen firewall options secure a zone by inspecting, and then allowing or denying, all connection attempts that require crossing an interface from and to that zone. To protect against TCP attacks from other zones, you can enable defense mechanisms known as SCREEN attack protections that detect and deflect the TCP packet attack. Common TCP packet attacks are SYN floods, packet fragments, FIN bit with ACK Bit set, SYN and FIN bits set, TCP packets without flags, and UDP floods. For details on these attack types, see the NetScreen ScreenOS 5.0 Concepts & Examples Guide.

When you set options that detect and block these attacks, the device generates a log and sends it to the Log Viewer.

To configure blocking of common TCP attacks to generate SCREEN attack log entries:

1. In the Navigation Tree, click Device Manager and select FW/VPN Devices to display a list of available devices. Select a device and click the Edit icon. Security Manager displays the device configuration for the device.

2. Select Network > Zones to display the Zone configuration. Double-click a zone to display the Predefined Zone dialog box.

3. Select Screen. Security Manager displays the Predefined Zone - Screen dialog box. The Screen dialog box contains five tabs, as described below.

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flood Defense</td>
<td>Enables you to manage attacks that overwhelm the device with large numbers or floods of certain packet types.</td>
</tr>
<tr>
<td>TCP/IP Anomalies</td>
<td>Enables you to manage SYN and SYN-ACK-ACK attacks.</td>
</tr>
<tr>
<td>IP Option Anomalies</td>
<td>Enables you to set options that provide IP-related protections.</td>
</tr>
<tr>
<td>Block HTTP Components</td>
<td>Enables you to detect and block component-level attacks.</td>
</tr>
<tr>
<td>MS Windows Defense</td>
<td>Enables you to detect and block Windows attacks.</td>
</tr>
<tr>
<td>Denial of Service Defense</td>
<td>Enables you to detect and block Denial of Service (DoS) attacks.</td>
</tr>
<tr>
<td>Scan/Spoo/Sweep Defense</td>
<td>Enables you to detect and block systems scans and identify spoofing attacks.</td>
</tr>
</tbody>
</table>
For a brief description of common SCREEN attacks, refer to the following table:

<table>
<thead>
<tr>
<th>Attack</th>
<th>What it means</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYN Attack</td>
<td>A flooding of SYN packets that overwhelms the network resulting in a denial of service (DoS) response to all packets by the port where the attack occurred.</td>
</tr>
<tr>
<td>Fragments</td>
<td>Reduced portions of an attack packet that in complete form would be recognized by the firewall policy. By disassembling into smaller, non-defined packet portions, the fragments go unrecognized by the policy and reassemble into the whole attack packet after they have entered the device where they can degrade data and cause port and device interruption.</td>
</tr>
<tr>
<td>FIN Bit With No ACK Bit</td>
<td>An instance where a TCP packet occurs with the FIN flag set, but with the ACK bit not set. TCP packets with the FIN flag normally also have the ACK bit set. This condition causes the NetScreen FW/VPN device to drop the packet.</td>
</tr>
<tr>
<td>SYN and FIN Bits Set</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. The attacker can then use any known system vulnerabilities for further attacks.</td>
</tr>
<tr>
<td>TCP Packet Without Flag</td>
<td>TCP packets are normally sent with at least one bit in the flag field set. This condition causes the NetScreen FW/VPN device to drop a packet.</td>
</tr>
<tr>
<td>Deny UDP Flood</td>
<td>UDP packets overlaid a system with so many packets that the system can no longer process.</td>
</tr>
</tbody>
</table>

After you have updated the device with the edited device configuration, the Log Viewer Misc. column displays a text message containing the severity level.

**Configuring Self Logs**

Self log entries display information dropped by the NetScreen FW/VPN device or on traffic that terminates on the device. A self log includes information on the date and time when the packet was dropped, the source address of the packet, the destination address of the packet, the duration for which the packet has been active, and the service associated with the packet.

Any packet that terminates at the device generates a self log. Any PC that can ping the device will generate a packet that terminates on the device. Telnet, Ping, BGP, OSPF. Logs all packets that terminate at the box. To configure self log entries:

1. In the Navigation Tree, double-click Device Manager to display a list of available devices. Select a device and click the Edit icon. Security Manager displays the device configuration dialog box.
2. Select Report Settings > General. Click the Firewall Options tab and configure the following settings:

<table>
<thead>
<tr>
<th>Checkbox</th>
<th>What it means</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log ICMP Packets to Self</td>
<td>Indicates whether you want to log ping packets.</td>
</tr>
<tr>
<td>Log IKE Packets to Self</td>
<td>When you want to negotiate an IKE key, the VPN client has to talk to the NetScreen FW/VPN device. Controls whether you want to keep a record of an IKE type self log.</td>
</tr>
<tr>
<td>Log SNMP Packets to Self</td>
<td>Controls whether or not you keep a record of an SNMP type self log.</td>
</tr>
<tr>
<td>Log Multicast Packets to Self</td>
<td>Controls whether or not you keep a record of a multicast packet-generated self log.</td>
</tr>
</tbody>
</table>

After you have updated the device with the edited device configuration, the Log Viewer displays the following columns of information for a custom self log:

- Source
- Destination
- Services

**Forwarding Logs to Other Destinations**

You can forward log entries generated by an individual device to specified destinations, as detailed below:

<table>
<thead>
<tr>
<th>Log Destination</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console</td>
<td>The PC you use to view log entries in the logging tools in Security Manager.</td>
</tr>
<tr>
<td>Email</td>
<td>An Email server to which you want log information forwarded.</td>
</tr>
<tr>
<td>Syslog</td>
<td>The syslog facility on the Device Server.</td>
</tr>
<tr>
<td>WebTrends</td>
<td>A WebTrends server to which you want log entries forwarded.</td>
</tr>
<tr>
<td>NSM</td>
<td>The Security Manager server.</td>
</tr>
<tr>
<td>PCMCIA</td>
<td>A PCMCIA device to which you want log entries forwarded.</td>
</tr>
<tr>
<td>Internal</td>
<td>An destination within the current device to which you want log entries forwarded.</td>
</tr>
</tbody>
</table>

The following sections detail how to configure a device to forward log entries to specific destinations. For details on configuring devices and device Reporting Settings, see Chapter 4, “Configuring Devices”.

**Directing Logs to a Console Destination**

You can specify both emergency-level and information-level log entries to be sent to the console destination. To set a severity level filter for a console destination:
1. In the Navigation Tree, click Device Manager and select FW/VPN Devices to display a list of available FW/VPN devices. Double-click a device in the main display area to display its device configuration.

2. In the device configuration, select Report Settings > General. Security Manager displays the General dialog box. The Console tab appears by default.

3. Select the severity level that you want to use as a criteria for forwarding only log entries that have that severity level to the destination you selected.

### Directing Logs to an SNMP Destination

To direct log entries to an SNMP destination, click the SNMP option. Security Manager displays the SNMP dialog box. Type appropriate data into the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Name</td>
<td>The name of the device for which you are generating SNMP status.</td>
</tr>
<tr>
<td>Contact Person</td>
<td>The name of the network administrator who manages the device.</td>
</tr>
<tr>
<td>Location</td>
<td>The location of the device.</td>
</tr>
<tr>
<td>Listen Port</td>
<td>The number of the port assigned to monitor SNMP traffic.</td>
</tr>
<tr>
<td>Trap Port</td>
<td>The number of the port assigned to transmit traps that have been generated by an SNMP alarm, threshold violation, or error.</td>
</tr>
<tr>
<td>Enable Authentication</td>
<td>Specifies whether you want to generate a trap if a packet fails to be authenticated when attempting to enter the device.</td>
</tr>
<tr>
<td>Fail Trap</td>
<td>Specifies whether you want to generate a trap if a packet fails to be authenticated when attempting to enter the device.</td>
</tr>
</tbody>
</table>

Community names enable you to set a string that requires a user to match as they attempt to gain access to the device. Click the Add icon to create an SNMP community name for the device and configure the settings associated with it. The following table details the settings you need to configure to create a community name.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Community-Name</td>
<td>The string that identifies the community name to be used to authorize users attempting to enter the device.</td>
</tr>
<tr>
<td>Access-Mode</td>
<td>Indicates the level of privilege a user has to set data on the device.</td>
</tr>
<tr>
<td>Trap-Mode</td>
<td>Indicates whether an administrator set the device to generate traps.</td>
</tr>
<tr>
<td>Traffic</td>
<td>Indicates whether the device accepts traffic from the source interface.</td>
</tr>
</tbody>
</table>

You can set severity levels for SNMP destinations by clicking the Log Settings option under the Report Settings option in the Navigation Tree. Then click the SNMP Tab and select the desired severity checkbox.
**Directing Logs to a Syslog Server**

To send log entries to a Syslog server, click the Syslog option. Security Manager displays the Syslog dialog box. Enter appropriate data into the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Syslog Messages</td>
<td>Initiates the logging of system event messages to the Syslog.</td>
</tr>
<tr>
<td>Port Number</td>
<td>Indicates the port number from where the messages are sent to the Syslog.</td>
</tr>
<tr>
<td>Use Trust Zone Interface as Source IF for VPN</td>
<td>Specifies using the interface mapped to the Trust zone as the source of traffic for a VPN.</td>
</tr>
<tr>
<td>Include Traffic Log</td>
<td>Specifies that all traffic log events are included as part of the messages sent to the syslog.</td>
</tr>
<tr>
<td>Config Host</td>
<td>Indicates the name of the host device.</td>
</tr>
</tbody>
</table>

You can set severity levels for Syslog destinations by clicking the Log Settings option under the Report Settings option in the Navigation Tree. Then click the Syslog Tab and click on the desired severity checkbox.

**Directing Logs to an Email Server**

To send log entries to an Email server, click the Email option. Security Manager displays the Email dialog box. Enter appropriate data into the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Notification for Alarms</td>
<td>Directs the device to forward notifications to the specified Email server when Security Manager receives an alarm.</td>
</tr>
<tr>
<td>Include Traffic Log</td>
<td>Directs the device to forward an incoming log to the specified Email server when Security Manager receives the log.</td>
</tr>
<tr>
<td>SMTP Server Name</td>
<td>The name of the Simple Mail Transfer Protocol server to which you want Security Manager to forward log entries.</td>
</tr>
<tr>
<td>E-mail Address 1</td>
<td>The primary email address to which you want Security Manager to forward log entries.</td>
</tr>
<tr>
<td>E-mail Address 2</td>
<td>The secondary email address to which you want Security Manager to forward log entries.</td>
</tr>
</tbody>
</table>

You can set severity levels for Email destinations by clicking the Log Settings option under the Report Settings option in the Navigation Tree. Then click the Email Tab and click on the desired severity checkbox.
Configuring Logging

Directing Data to a WebTrends Server

To send log entries to a WebTrends server, click the WebTrends option. Security Manager displays the WebTrends dialog box. Enter appropriate data into the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable WebTrends Message</td>
<td>Directs Security Manager to forward a log to the WebTrends server.</td>
</tr>
<tr>
<td>WebTrends Host Name</td>
<td>The name of the WebTrends server.</td>
</tr>
<tr>
<td>Port</td>
<td>Specifies the port number through which the device sends the log to the WebTrends server.</td>
</tr>
<tr>
<td>Use Trust Zone Interface as Source IP for VPN</td>
<td>Directs the device to use the interface mapped to the trust zone as the location for the Virtual Private Network over which the packets are forwarded to the WebTrends server.</td>
</tr>
</tbody>
</table>

You can set severity levels for WebTrends destinations by clicking the Log Settings option under the Report Settings option in the Navigation Tree. Then click the WebTrends Tab and click on the desired severity checkbox.

Configuring Logging in Firewall Rules

The following sections detail how to configure logging in your firewall rules.

For details on creating firewall policies and working with firewall rules, see Chapter 8, “Configuring Firewall Policies”.

Configuring Traffic Logs

Every time the NetScreen FW/VPN device receives a packet that matches a firewall rule, the device can generate a traffic log if logging is enabled in the firewall policy for that device. To configure traffic log entries, you need to create a firewall rules that searches for a specific matching condition. The following table describes the various matching conditions used to configure a traffic log.

<table>
<thead>
<tr>
<th>Condition</th>
<th>What It Is</th>
</tr>
</thead>
<tbody>
<tr>
<td>From Zone</td>
<td>Indicates the condition for generating a traffic log is a specified zone that sends a packet attempting to enter the NetScreen FW/VPN device.</td>
</tr>
<tr>
<td>Source</td>
<td>Indicates the condition for generating a traffic log is a specified source address that sends a packet attempting to enter the NetScreen FW/VPN device.</td>
</tr>
<tr>
<td>To Zone</td>
<td>Indicates the condition for generating a traffic log is a specified zone to which a packet is targeted when entering the NetScreen FW/VPN device.</td>
</tr>
<tr>
<td>Destination</td>
<td>Indicates the condition for generating a traffic log is a specified destination address to which a packet is targeted when entering the device.</td>
</tr>
</tbody>
</table>
To configure a firewall rule to generate traffic log entries for matching traffic:

1. In the Navigation Tree, click Policy Manager and select a firewall policy.
2. Right-click the Rule Options column of the rule and select Log/Count. Security Manager displays the Configure Log/Count dialog box.
   - To enable the rule to generate log entries, select Logging.
   - To set log entries generated from the rule to display alert flags in the Log Viewer, select Alert.
   - To activate selection of throughput levels that create limits for the number log entries that can enter the Log Viewer, select Counting.
   - To direct Security Manager to generate an alarm if the count value is surpassed, select Alarm Enabled.
   - To create the count value, select a Bytes/Second or Kilobytes/Minute value. This value indicates an upper limit for the amount of bytes or kilobytes of log data that can enter the Log Viewer.
3. Click OK to return to the firewall policy.

After you have updated your managed devices to use the edited policy, the Log Viewer displays traffic log entries with the following columns of information:

- From Zone
- To Zone
- Source IP
- Destination IP
- Action
- Service

Traffic log entries are only for firewall-related events. Deep Inspection events do not generate traffic log entries.
Configuring Alarm Logs

To configure a device to generate alarm log entries:

1. In the Navigation Tree, click Policy Manager and select a firewall policy.
2. Right-click in the Rule Options column of the rule and select Log/Count. Security Manager displays the Configure Log/Count dialog box.
   - To activate selection of throughput levels that create limits for the number log entries that can enter the Log Viewer, select Counting.
   - To direct Security Manager to generate an alarm if the count value is surpassed, select Alarm Enabled (You must enable Counting before you can configure alarms).
   - To create the count value, select a Bytes/Second or Kilobytes/Minute value. This value indicates an upper limit for the amount of bytes or kilobytes of log data that can enter the Log Viewer.
3. Click OK to return to the Log/Count tab.
4. Select the Traffic Shaping tab, then select Enabled to configure traffic shaping for the rule:
   - To create a minimum amount of ensured throughput for packets, select Guaranteed Bandwidth and select a value
   - To determine the priority or relative weight that alarm log entries will have relative to other log entries, select Priority and select a value.
   - To determine the upper limit of throughput provided for log entries generated by Security Manager, select Maximum Bandwidth and a value.
5. Click OK to return to the firewall policy. Save the firewall policy and update the managed devices that use that policy.

After you have updated the device with the edited policy, the Log Viewer displays the following columns of information for an alarm log:

- To Zone
- From Zone
- Source IP
- Destination IP
- Threshold (displayed in the Misc column of the Log Viewer)

Configuring Anomaly Logs

Anomaly attack checking are features that verify that traffic of a designated protocol type is really of the type it indicates. If the packets of a suggested protocol type do not behave or demonstrate attributes of that protocol type (for example, HTTP), they may be spoofing and attempting to enter the network as an intruder.

Protocol anomalies are an attack type. When the device detects a protocol anomaly attack, Security Manager sends a log to the Log Viewer. You need to specify the type of anomaly you want Security Manager to check for and issue a log for instances when the device detects the specified anomaly type.
1. In the Navigation Tree, click Policy Manager and select a firewall policy.
2. Right-click in the Rule Options column of the rule and select Attack Protection. Security Manager displays the Attack Protection dialog box. The Attacks tab displays by default.
3. Select anomaly attacks from the list. Hold your mouse cursor over each attack to determine which attacks are anomaly attacks.
4. Click OK to return to the firewall policy.
5. Save the firewall policy and update the managed devices that use that policy.

After you have updated the device with the edited policy, the Log Viewer displays the following columns of information for an anomaly log:

- Subcategory (This information displays the actual attack type. Each log category has a number of subcategories)
- Action (Different actions than traffic log entries: close, close client, drop packets)
- Severity
- Source
- Destination
- Zones
- Service

### Configuring Signature Logs

Signatures are patterns and pieces of information that an attack leaves on the device after it entered the device. A typical piece of information the attack leaves behind is a source address of the device that generated the attack.

NetScreen maintains a list of many of the common signatures discovered left on various networks during the past few years. Signatures are collected and distributed to the networking community by various means, often bulletins indicating that one has been traced on a given network.

You can configure a NetScreen FW/VPN device to generate a log entry and send it to the Log Viewer when the device detects a signature preconfigured as a logging condition using Security Manager.

To configure a device to generate signature log entries:

1. In the Navigation Tree, click Policy Manager and select a firewall policy.
2. Right-click in the Rule Options column of the rule and select Attack Protection. Security Manager displays the Attack Protection dialog box. The Attacks tab displays by default.
3. Select signature attacks from the list. Hold your mouse cursor over each attack to determine which attacks are signature attacks.
4. Click OK to return to the firewall policy.
5. Save the firewall policy and update the managed devices that use that policy.
After you have updated the device with the edited policy, the Log Viewer displays the following columns of information for a signature log:

- Subcategory
- Actions (Attack -> Options)
- Severity
- Service
- Source
- Destination
- Zones

Configuring Custom Attack Logs

New attacks are created constantly, and can enter your networks undetected before the industry can learn of the attack type and alert the networking community about it. For new attacks, NetScreen may not provide a preset signature condition that your network attempts to block. For these types of attacks, you can create a custom attack filter.

A custom attack filter is a signature condition that you create to detect patterns that an attack leaves on a device on your network for which there is no coverage for in the current list of attack types that NetScreen provides.

To configure a firewall rule to generate custom log entries for matching traffic:

1. Create a custom signature Attack Object. For details, see “Creating Custom Attack Objects” on page 214.
2. In the Navigation Tree, click Policy Manager and select a firewall policy.
3. Right-click in the Rule Options column of the rule and select Attack Protection. Security Manager displays the Attack Protection dialog box. The Attacks tab displays by default.
4. Select your custom attack from the list.
5. Click OK to return to the firewall policy.
6. Save the firewall policy and update the managed devices that use that policy.

After you have updated the device with the edited policy, the Log Viewer displays the following columns of information for a custom attack log:

- Subcategory
- Severity
- Action (Attack - Options)
- Zone
- Source
- Destination
- Service
Configuring the GUI Server for Logging

High-traffic networks can produce a lot of log entries. You can print or export, or purge your log entries to help keep them organized. The GUI Server organizes log data for all managed devices. You can configure the GUI Server to perform actions (syslog, export, alarm, etc.) on that log data based on the criteria you specify. To activate log actions on the GUI Server, you must configure:

- **Log criteria.** The criteria determines the category, subcategory, and severity for a matching log entry. If a log entry meets the specified criteria, it is considered qualified, and Security Manager takes the specified log action.
- **Log action settings.** These settings determine how the GUI Server handles qualified log entries.

Configuring Log Actions

To export to XML, CSV, SNMP, SMTP, Syslog, or script, configure the GUI Server Log Actions to export log entries to the specified format.

You can configure the following log actions:

- Send log entries to your syslog server
- Send log entries to your SNMP server
- Export log entries to .CSV or .XML file
- Email alarms using your SMTP server

The following sections detail log action settings.

**Syslog**

To enable the GUI Server to send qualified log entries to your syslog server, specify the IP address or host name for the syslog server.

**SNMP**

To enable the GUI Server to send log entries to an SNMP server, configure the following SNMP settings:

- **SNMP Manager.** Specify the IP address or host name of the SNMP server that 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.

Security Manager exports all qualified log entries to the specified SNMP server.

**CSV**

To enable the GUI Server to export log entries in CSV format, configure the CSV settings:

- **File Path.** The path you want log entries exported to in .CSV format
- **Print Header.** Export column headers to .CSV format.

Security Manager exports all qualified log entries to CSV; each log becomes a CSV record.
**XML**

To enable the GUI Server to export log entries in XML format, configure the file path you want log entries exported to in XML format.

Security Manager exports all qualified log entries to XML; each log becomes an XML record, which you can open in most Web browsers.

**Email**

To enable the GUI Server to send email alarms to a Simple Mail Transfer Protocol (SMTP) email file on an SMTP server, specify the SMTP settings:

- **SMTP Server**: The mail server (IP address or host name) that receives email alarms.
- **From Email Address**: The server (IP address or host name) 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.

Security Manager sends email alarms generated by qualified log entries to the specified SMTP server.

**Log Criteria**

Click the Log Criteria tab to specify the type of log entries that trigger the actions you set in the Log Actions tab. To add a new criteria, right-click and select Add Criteria, then configure the following settings.

**Category, Subcategory, & Severity**

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. Next, select a severity of log entry.

**Other Log Types**

Some log types are always enabled and do not need to be configured. These log types appear in the Log Viewer and can provide valuable information about your network.

**Information Logs**

Information log entries refer to basic administrative events that occur when a network administrator changes basic settings on a managed device. When the device detects a change to one of these settings, the device generates a log entry and includes information about the change.
You do not need to configure any settings to generate information log entries. The tasks you perform that automatically generate these log entries include: logging into a device, logging out of a device, setting a new password for the device, issuing a key value for the device, and entering an MD5 authentication password to enter a device.

For information log entries, the Log Viewer Detail column displays a text message detailing the severity level.

**Configuration Logs**

Any event that changes the configuration on the device is a configuration log. Specifically, any command issued that the ScreenOS `get config` command statement captures and displays in ScreenOS generates a configuration log. Note that when you configure a setting in Security Manager, the Data Model registers the configuration and converts it into comparable ScreenOS command statements when the configuration is sent to the device. So any configuration you set in Security Manager written to the device generates a configuration log.

For configuration log entries, the Log Viewer Detail column displays a text message detailing the severity level.
**Using the Log Viewer**

The Log Viewer displays log entries generated by a NetScreen FW/VPN device when traffic matches a firewall or VPN rule, or when an event occurs that matches a predefined set of conditions. Use the Log Viewer to:

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

**About the Log Viewer**

Before beginning to learn more about the Log Viewer, review the following figure of the Log Viewer and column descriptions to better understand this traffic analysis tool.
Log Viewer Columns

The Log Viewer contains the following 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>Default</td>
<td>Indicates the date and the time that the Log Viewer received the log entry.</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>Default</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 over which the packet associated with the generated log entry was transmitted.</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 sub-category of the log you are viewing. A sub-category is an attack type.</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>Field</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Action</td>
<td>Indicates whether an action occurred in response to the event that generated the log.</td>
<td></td>
</tr>
<tr>
<td>Alert</td>
<td>Indicates whether an alert flag was generated in response to the event that generated the log.</td>
<td></td>
</tr>
<tr>
<td>App</td>
<td>Indicates the application associated with the current log.</td>
<td></td>
</tr>
<tr>
<td>Bytes In</td>
<td>Indicates the number of bytes that comprised the log data entering the Log Viewer.</td>
<td></td>
</tr>
<tr>
<td>Bytes Out</td>
<td>Indicates the number of bytes that comprised the log data being transmitted from the Log Viewer.</td>
<td></td>
</tr>
<tr>
<td>Bytes Total</td>
<td>The sum of the number of bytes transmitted and received by the Log Viewer.</td>
<td></td>
</tr>
<tr>
<td>Device</td>
<td>Indicates the IP address of the device that generated the current log.</td>
<td></td>
</tr>
<tr>
<td>Device Domain</td>
<td>Indicates the name of the domain in which the device resides.</td>
<td></td>
</tr>
<tr>
<td>Domain Ver</td>
<td>Indicates the version number of the device.</td>
<td></td>
</tr>
<tr>
<td>Elapsed Secs</td>
<td>The number of seconds that have elapsed since the beginning of the current session.</td>
<td></td>
</tr>
<tr>
<td>From External</td>
<td>Specifies if the packet that generated this log came from an untrusted network.</td>
<td></td>
</tr>
<tr>
<td>Has Log Action</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>
<td></td>
</tr>
<tr>
<td>Has Packet Data</td>
<td>Specifies if this log has associated packet data.</td>
<td></td>
</tr>
<tr>
<td>In Eth</td>
<td>The name of the Ethernet interface that receives packets transmitted from an external device.</td>
<td></td>
</tr>
<tr>
<td>Misc</td>
<td>A miscellaneous string associated with the current log.</td>
<td></td>
</tr>
<tr>
<td>NAT Dst Port</td>
<td>A destination port associated with the packet that has generated the log that has also undergone a network address translation.</td>
<td></td>
</tr>
<tr>
<td>NAT Src Port</td>
<td>A source port associated with the packet that has generated the log that has also undergone a network address translation.</td>
<td></td>
</tr>
<tr>
<td>NAT Dst Addr</td>
<td>A destination address associated with the packet that generated the log that has also undergone a network address translation.</td>
<td></td>
</tr>
<tr>
<td>NAT Src Addr</td>
<td>The source address associated with the packet that generated the log that has also undergone a network address translation.</td>
<td></td>
</tr>
<tr>
<td>Out Eth</td>
<td>The name of the Ethernet interface that transmits packets to an external device.</td>
<td></td>
</tr>
<tr>
<td>Packets In</td>
<td>Specifies the number of received packets for a given session on the current port.</td>
<td></td>
</tr>
<tr>
<td>Packets Out</td>
<td>Specifies the number of transmitted packets for a given session on the current port.</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 11 Logging

The bottom portion of the Log Viewer is the Log Viewer Summary and contains two tabs and two regions. The following table describes the tabs.

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Provides a description of the attack associated with the log entry that you have selected and other data associated with it.</td>
</tr>
<tr>
<td>All Fields</td>
<td>Provides a condensed text view of the log entry that you have selected.</td>
</tr>
</tbody>
</table>

The Summary Tab is the default tab and contains two default regions, the Attack region which provides an attack description of the log you have selected and the Variable Data region which provides additional data on the attack.

The Summary Tab enables you to view the value of each sub-category column of the Log Viewer for log that do not signify attacks.

A sample view of an event summary is shown in the following figure.
Using the Log Viewer

Note the attack description in the Attack Region to the left. The following table details the data in the Variable Data region to the right.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Type</td>
<td>Displays a code that identifies the hardware platform on which you are working.</td>
</tr>
<tr>
<td>Protocol Type</td>
<td>Displays the protocol type for which the device has been configured.</td>
</tr>
<tr>
<td>Hardware Length</td>
<td>Displays the length of the hardware type.</td>
</tr>
<tr>
<td>Protocol Length</td>
<td>Indicates the length of the protocol type.</td>
</tr>
</tbody>
</table>

Managing Logs

Because the Log Viewer may receive hundreds or even thousands of log entries each day, you may spend too much time trying to locate the log entries for which you are searching. For example, if you search for a log entry generated by a port scan attack (TCP Port Scan) that occurred during the past several days, you might have to scroll through 20 or 30 screens in the Log Viewer to find it. You could easily overlook a log given the amount of detail that the Log Viewer displays.

Security Manager provides several event viewing techniques that make the process of locating log more manageable. Each technique has benefits to it, but each also has limitations to it. Try to combine various event viewing techniques to make event location as efficient as possible. Also use only an event viewing technique that seems appropriate. The following table details the event searching techniques provided by Security Manager.

<table>
<thead>
<tr>
<th>Tool</th>
<th>Description</th>
<th>Benefit</th>
</tr>
</thead>
</table>
| Flags          | A symbol that you use to tag a specific event that you have found that you want to return to at a later point. By leaving a distinct tag on the entry, it will stand out from other entries when you return to the log. | • Manual assigning of flags gives administrator 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 tool that searches for a log based on a character string believed to be in the reported event. | • Enables you to locate a specific event quickly without having to know many details about it, for example, timestamp or address information.  
• Enables you to skip from one relevant event to another, avoiding scrolling. |
Flags enable you to identify certain types of events that are being sent to the log by labeling them with certain types of symbols indicating a severity level. By applying a flag to each log, you can make the log easily stand out more from the hundreds of log entries that display in the Log Viewer. The following table displays a list of log filter symbols.

<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>
<tr>
<td>Assigned</td>
<td></td>
<td>Information</td>
</tr>
<tr>
<td>False Positive</td>
<td></td>
<td>Information</td>
</tr>
</tbody>
</table>
Using Report Manager, you can generate a report that displays the count of all log entries that contain a flag.

Using the Find Utility

The Find utility behaves similarly to the Filter utility in Security Manager. The difference between the two is the Find utility seeks out the next iteration (down) of a value you are searching for, from the point where you are in the Log Viewer. You can use the Find utility at both the column level and the cell level. To use the Find utility on the Column level, right-click the column header for which you want to use as criteria to find a log. To use the Find utility on the cell level, right-click the cell. You can search for all log entries that do not contain the specified data by selecting Negate.

Locating Logs By ID Number

You can also locate a log by using a search utility that brings you quickly to a log by specifying a log ID number. This utility is a helpful way to locate log entries when you already know the ID number of the log, generally, when you have already viewed the log and have recorded the number, and you want to return to the log for a second view. To use the find utility, click the Go To Log ID option in the Edit menu. Security Manager displays the Go To Log ID dialog box. Type the log ID number in the field in the dialog box and click Ok to locate the log.

Using Filters

You set filters for specific columns or cells in the Log Viewer. Each column has its own data type and environment that make filtering distinct for each environment.

Filtering by Log Viewer Cell

Filters applied to cells affect only the content in that cell’s column. Right-click the cell you want to filter on 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.

**Filtering by Log Viewer Column**

You can also filter on columns. Two useful types of filtering are available for you in the Log Viewer.

- **Time-Based Filtering.** Time-based filtering pertains to the types of filters that you set up that use time and date information as criteria for screening log entries entering the Log Viewer. Time-based filtering enables you to direct the Log Viewer to display only events that occurred within a specified time period.
- **Event-Based Filtering.** Event-based filtering pertains to the types of filters that you set up that use attack types as criteria for screening log entries entering the Log Viewer. Event-based filtering enables you to direct the Log Viewer to display only events that have been generated by attacks associated with them.

The Log Viewer displays the following event types:

<table>
<thead>
<tr>
<th>Event</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm</td>
<td>When the detects a violation of a security policy rule with an alarm threshold.</td>
</tr>
<tr>
<td>Anomaly</td>
<td>When Security Manager detects an that matches a protocol anomaly attack group.</td>
</tr>
<tr>
<td>Config</td>
<td>When a configuration or operational state changed in Security Manager.</td>
</tr>
<tr>
<td>Custom</td>
<td>When Security Manager detects an event that matches a user-defined signature.</td>
</tr>
<tr>
<td>Info</td>
<td>Details general system information.</td>
</tr>
<tr>
<td>Self</td>
<td>When Security Manager detects an event that is non-traffic related.</td>
</tr>
<tr>
<td>Signature</td>
<td>When Security Manager detects an event that matches an attack pattern.</td>
</tr>
<tr>
<td>Traffic</td>
<td>When Security Manager detects a traffic-based detection violation.</td>
</tr>
<tr>
<td>Screen</td>
<td>When Security Manager detects a NetScreen Screen-level attack.</td>
</tr>
<tr>
<td>Implicit</td>
<td>Contains implicit attack signatures.</td>
</tr>
</tbody>
</table>
Setting a Category Filter

The Log Viewer contains two columns that pertain to categories: Category and Sub-Category. The category simply pertains to the log type described in the section about log types earlier in this chapter. For each log type or category, Security Manager provides several or even many subcategories which specify the log type even more finely. For example, the category may specify a traffic log, but when you look at the sub-category, it may indicate a more specific type of traffic log.

The following tables display subcategories mapped to several common categories. For subcategories for configuration log entries, see the following table.

<table>
<thead>
<tr>
<th>Subcategory</th>
<th>Subcategory</th>
<th>Subcategory</th>
<th>Subcategory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>DNS-Rep</td>
<td>Policy Unload</td>
<td>SSH</td>
</tr>
<tr>
<td>Admin</td>
<td>Erase</td>
<td>PPP</td>
<td>SSL</td>
</tr>
<tr>
<td>Auth</td>
<td>Firewall</td>
<td>PPPoE</td>
<td>Startup</td>
</tr>
<tr>
<td>BGP</td>
<td>Hostname</td>
<td>Route</td>
<td>Syslog</td>
</tr>
<tr>
<td>CLS</td>
<td>Interface</td>
<td>Route Map</td>
<td>URL</td>
</tr>
<tr>
<td>Clock</td>
<td>IDS</td>
<td>Schedule</td>
<td>User</td>
</tr>
<tr>
<td>CMS</td>
<td>MIP</td>
<td>Service</td>
<td>VIP</td>
</tr>
<tr>
<td>Console</td>
<td>NSRP</td>
<td>Session</td>
<td>VPN</td>
</tr>
<tr>
<td>DHCP CLI</td>
<td>OSPF</td>
<td>Shutdown</td>
<td>Vsys</td>
</tr>
<tr>
<td>DHCP IP</td>
<td>Others</td>
<td>SNMP</td>
<td>Zone</td>
</tr>
<tr>
<td>DHCP Opt</td>
<td>PKI</td>
<td>Shaper</td>
<td></td>
</tr>
<tr>
<td>DIP</td>
<td>Policy</td>
<td>SME</td>
<td></td>
</tr>
<tr>
<td>DNS</td>
<td>Policy Load</td>
<td>Softkey</td>
<td></td>
</tr>
</tbody>
</table>

For subcategories for information log entries, see the following table:

<table>
<thead>
<tr>
<th>Subcategory</th>
<th>Subcategory</th>
<th>Subcategory</th>
<th>Subcategory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link Status</td>
<td>System Status</td>
<td>DNS</td>
<td>DHCP CLI</td>
</tr>
<tr>
<td>Others</td>
<td>NSRP Status</td>
<td>Clock</td>
<td>Dev Connect</td>
</tr>
<tr>
<td>LB_SRV_Status</td>
<td>URL Block</td>
<td>Ping</td>
<td>Dev Disconnect</td>
</tr>
<tr>
<td>Login/Logout</td>
<td>SNMP</td>
<td>LB Server Up</td>
<td>No Heartbeat</td>
</tr>
<tr>
<td>Password Change</td>
<td>Authorization State Change</td>
<td>Log Cleared</td>
<td>PPPoE</td>
</tr>
<tr>
<td>Username Change</td>
<td>NUUser Status</td>
<td>PKI</td>
<td>PPP</td>
</tr>
<tr>
<td>Authorization Failed</td>
<td>DHCP Server</td>
<td>VPN</td>
<td>SSL</td>
</tr>
<tr>
<td>Authorization Success</td>
<td>SSH</td>
<td>Generic</td>
<td>OSPF</td>
</tr>
<tr>
<td>Authorization Timeout</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
For subcategories for alarm log entries, see the following table:

<table>
<thead>
<tr>
<th>Subcategory</th>
<th>Subcategory</th>
<th>Subcategory</th>
<th>Subcategory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Others</td>
<td>DHCP</td>
<td>NSRP VSD Backup</td>
<td>NSRP VSD 2nd Path Reply</td>
</tr>
<tr>
<td>Hardware</td>
<td>Device Dead</td>
<td>NSRP VSD Ineligible</td>
<td>NSRP RTO Duplicate</td>
</tr>
<tr>
<td>User Block</td>
<td>Memory Low</td>
<td>NSRP TrackIP Failed</td>
<td>NSRP IP Duplicate Master</td>
</tr>
<tr>
<td>DNS Host</td>
<td>CPU Usage High</td>
<td>NSRP TrackIP Failover</td>
<td>Route Sys Entry Ex</td>
</tr>
<tr>
<td>Log Overflow</td>
<td>IP Conflict</td>
<td>NSRP Inconsistent Configuration</td>
<td>Route VR Entry Ex</td>
</tr>
<tr>
<td>VPN</td>
<td>VPN Status Up</td>
<td>NSRP VSD Init</td>
<td>SSH</td>
</tr>
<tr>
<td>NSRP Status</td>
<td>VPN Status Down</td>
<td>NSRP VSD Master</td>
<td>Session Allocated</td>
</tr>
<tr>
<td>LB Server Down</td>
<td>NSRP RTO Up</td>
<td>NSRP VSD PBackup</td>
<td>Route OSPF Hello Flood</td>
</tr>
<tr>
<td>Admin</td>
<td>NSRP RTO Down</td>
<td>NSRP VSD Inoperable</td>
<td>Route OSPF LSA Flood</td>
</tr>
<tr>
<td>PKI</td>
<td>NSRP TrackIP Success</td>
<td>NSRP VSD 2nd Path Required</td>
<td>Default</td>
</tr>
</tbody>
</table>

### Setting an Alert Filter

You can set a filter that displays only log entries based on whether the log contains an enabled or disabled alert. To create a filter that displays log entries based on a specific alert state, right-click the Alert column and right-click Filter option and then right-click the Edit option. Security Manager displays the Filter for Alert dialog box.

To display only log entries that contain a specified alert state:

- To display only log entries that have no alert state set, click the No Filter radio button and click Ok.
- To display only log entries that contain an enabled alert, click the On radio button and click Ok.
- To display only log entries that contain a disabled alert, click the Off radio button and click Ok.

### Setting a Flag Filter

You can set a filter that displays only log entries based on whether the log contains a specified flag type. To create a filter that displays log entries based on whether they contain a flag type, right-click the Flag column and right-click Filter option and then right-click the Edit option. Security Manager displays the Filter for User Flag dialog box.

- To display only log entries that contain a specified flag type, click one or several of the flag checkboxes and click Ok. Security Manager now displays only log entries that contain the flag types you checked.
- To display only log entries that do not contain a specified flag type, click one or several the flag checkboxes, click the Negate checkbox, and click Ok. Security Manager displays only log entries that do not contain the flag types you checked.
**Setting an Address Filter**

You can create a filter that displays only log entries that contain a specified source or destination address. To create a filter that displays log entries that contain a specified source or destination address, right-click either the Src Addr or Dst Addr column and right-click Filter option and then right-click the Edit option. Security Manager displays either the Filter for Src Addr or Filter for Dst Addr dialog boxes.

- To display only log entries that contain a specific source or destination address, click the field that contains the string “Click here to add address,” type a valid IP address and click Ok. Log Viewer now displays only log entries that contain the source or destination address you specified.
- To display only log entries that do not contain a specific source or destination address, click the field that contains the string “Click here to add address,” type a valid IP address, click the Negate checkbox, and click Ok. Log Viewer now displays only log entries that do not contain the source or destination address you specified.

**Setting a NAT Address Filter**

You can create a filter that displays only log entries that contain a specified Network Address Translation (NAT) destination or source address. To create a filter that displays log entries that contain a specified NAT destination or source address, right-click the NAT Src Addr or NAT Dst Addr columns and right-click Filter option and then right-click the Edit option. Security Manager displays either the Filter on “NAT Src Addr” or Filter for “NAT Dst Addr” dialog box.

- To display only log entries that contain a specific source or destination NAT address, click the field that contains the string “Click here to add address,” type a valid address that will undergo a network address translation (conversion of public address to a private address) and click Ok. Log Viewer now displays only log entries that contain the source or destination address you specified.
- To display only log entries that do not contain a specific source or destination NAT address, click the field that contains the string “Click here to add address,” type an IP address, click the Negate checkbox, and click Ok. Log Viewer now displays only log entries that do not contain the source or destination NAT address you specified.

**Setting a Protocol Filter**

You can create a filter that displays only log entries that contain a specified protocol type. A prototype is a utility that deploys a certain type of architecture that may be part of a log’s profile. To create a filter that displays log entries that contain a specified protocol type, right-click the Protocol column and right-click Filter option and then right-click the Edit option. Security Manager displays the Filter for Protocol dialog box.

- To display only log entries that contain a specific protocol, click a desired protocol checkbox and click Ok. Log Viewer now displays only log entries that contain the protocol you specified.
To display only log entries that do not contain a specific protocol, click a desired protocol checkbox, click the Negate checkbox, and click Ok. Log Viewer now displays only log entries that do not contain the protocol you specified.

**Setting a Domain Filter**

You can create a filter that displays only log entries pertaining to devices that reside in a specified domain. A domain is a region in Security Manager that contains specified collections of devices. Domains can be useful in grouping devices with like attributes, for example, similar roles, locations, or device families. To create a filter that displays only log entries associated with devices in specified domains, right-click the Device Domain column and right-click the Filter option and then right-click the Edit option. Security Manager displays the Filter for the Device Domain dialog box.

• To display only log entries associated with a specific domain, click a desired domain checkbox and click Ok. Log Viewer now displays only log entries associated with devices in the domain you specified.

• To display only log entries not associated with a specific domain, click a desired domain checkbox, click the Negate checkbox, and click Ok. Log Viewer now displays only log entries not associated with the domain you specified.

**Example: Log Filtering**

The following example details a scenario where you would use filtering techniques to locate events in the Log Viewer.

<table>
<thead>
<tr>
<th>Company Type/Node Distribution</th>
<th>NetScreen Hardware</th>
<th>Event Attributes</th>
<th>Filtering Strategy</th>
</tr>
</thead>
</table>
| Medium-sized ISP              | NetScreen-500 in the central office with each branch office containing a NetScreen-5XTs. | • Time of event  
• Type of event | Designating a dedicated NetScreen-5XT in each branch office to accept only log entries that meet time and attack type requirements. |

A medium-sized ISP divides its administration into districts with a central regional office designated and several regional cluster offices belonging to the central office. The ISP monitors its facilities using a client-server approach using a central console and NetScreen-500 in the central office and NetScreen-5XTs in each regional office logging local information and feeding it to a central database in the central office.

The monitoring is targeted at tracking people who are barred from the ISP and who have been recently denied entry. Information is sent from the cluster office of the denial to the central office responsible for that cluster office. The central regional office covers ISP activity in regional cluster offices. About a dozen regional offices work under the server in the central office.

In recent weeks, two types of attacks have been received at three of the cluster offices several times at roughly the same time of the day interfering with access to border crossing information on a local database.
The alarm is being logged specifically at Regional Office 1, at Regional Office 2 and Regional Office 3. The alarm is “URL Blocking Server Connection,” causing the computer system to crash and eliminating any data that has been stored up in the past day. To obtain more information about the alarms that have occurred during the past few days, specifically source IP address information, network administrators have configured a designated NetScreen-5XT at each of the cluster offices that specifically attempt to display events in the Log Viewer that meet the following conditions:

- Attacks that arrive for the previous week between 4 and 7 p.m.
- Attacks that contain only the URL Blocking Server Connection alarm.
- Attacks that are associated only with Port 80 (HTTP attacks)

To configure your system to display only event types with this data in your Log Viewer:

1. In the Navigation Tree, click Log Viewer to display the Log Viewer.
2. Right-click the Time Received column header to display the Time Received configuration popup menu.
3. Click Filter and click Edit to display the Filter for “time received” dialog box.

4. In the From region:
   - Select the From checkbox.
   - Select the date box and enter today’s date (for example, 4/17/03).
   - Select the time list box and select 4:00:00 PM.
5. In the To region:
   - Select the To checkbox.
   - Select the date box and enter a value that is one week from today's date (for example, 4/24/03).
   - Select the time list box and select 7:00:00 PM.

6. Right-click the header of the Attack column and specify both the HTTP:Overflow and Trojan:Wincrash attack types by selecting the appropriate checkboxes.

7. Right-click the header of the Dst Port column, click the To checkbox and specify, using the numeric listbox, a value of 80 to indicate that you want to check for all packets entering system port 80 on the device. HTTP and URL related attacks enter the device on port 80.

You have now configured Security Manager to display only events in the Log Viewer that occur between 4 and 7 p.m. that contain the HTTP:Overflow and Trojan:Wincrash attack types in them. If you receive them, you can now go to the Source Address column of the events and record the IP addresses of the locations that are generating the events, bringing you closer to identifying the perpetrators of the network attacks.

After you have configured the filter in the above example, you may want to save it and use it again if another identical instance sequence of attacks occurs. Additionally, you may want to modify it to apply it to a similar attack or sequence of attacks that has some differences with it. For example, you may want to filter attacks using the same port number and attack type, but occur at different times or have a different action associated with them in a policy.

To save the filter in the above example, click the Save As option in the File menu and type a filename to which you want to save the filter in the Save View dialog box. To import the filter, click the Import Filter option in the File menu. To make changes to the filter, right-click one of the cells or columns and change the values on the desired settings of the filter.

**Searching with Ranges**

The Log Viewer provides boolean filter operators to filter on any column. The following table details the Boolean operators used for filtering in the Log Viewer. The following columns support range searching.

- Time Received
- Bytes In
- Bytes Out
- Bytes Total
- Source Port
- Destination Port
Working with Ranges in the Time Received Column

You can specify a range for when filtering for log that only meet the criteria of the Log Viewer receiving the log at time within the range. To specify a range so that the Log Viewer displays only log entries that arrive at the Log Viewer within the range of a specified starting and ending time:

1. Right-click the Time Received column and right-click Filter option and then right-click the Edit option. Security Manager displays the Filter for Time Received dialog box.
2. To display only log entries that arrive at the Log Viewer within a specified time range, perform one of the following steps:
   - To filter on log entries arriving only after a specified beginning time, click the From checkbox, click the From list box, and select a date and time.
   - To filter on log entries arriving only before a specified ending time, click the To checkbox, click the To list box, and select a date and time.
   - To filter on log entries arriving only between a specified beginning and ending time, click both the From and To checkboxes. Also, click both the From and To listboxes, and select a beginning time in the From listbox and an ending time in To listbox.
3. When you are satisfied with the time(s) you have entered, click Ok.

Working with Ranges in Bytes In/Out Columns

You can specify a range when filtering for log entries that only meet the criteria of a certain number of bytes either entering or leaving the device. To specify a range using the byte count as a criteria for log display:

1. Right-click either the Bytes In or Bytes Out column and right-click Filter option and then right-click the Edit option. Security Manager displays either the Filter for Bytes In or Filter for Bytes Out dialog box.
2. To display only log entries that contain a bytes received or bytes transmitted value that is within a range:
   - To filter on a minimum number of bytes, click in the From checkbox, click the From value list box and select a value.
   - To filter on a maximum number of bytes, click in the To checkbox, click the To value list box and select a value.
   - To filter on both a maximum and minimum number of bytes, click both the To and From checkboxes, click the appropriate list box and select a value.
3. To display only log entries that do not contain a bytes received or bytes transmitted value that is within a specified range, perform one of the following operations listed above and click the Negate checkbox.
4. When you are satisfied with the values you have entered, click Ok.
Working with Ranges in Port Number Columns

You can specify a range when filtering for log entries that only meet the criteria for either a destination or source port number either entering or leaving the device or both. To specify a range using the destination or source port number as a criteria for log display:

1. Right-click either the Src Port or Dst Port column. Security Manager displays either the Filter for Bytes In or Filter for Bytes Out dialog box.
2. To display only log entries that contain a source or destination port number that is within a range of values, perform one of the following steps.
   - To filter on a minimum port number value, click in the From checkbox, click the From value list box and select a value.
   - To filter on a maximum port number value, click in the To checkbox, click the To value list box and select a value.
   - To filter on both maximum and minimum port number values, select both To and From, then click the appropriate list box and select a value.
3. To display only log entries that do not contain a source or destination port number value that is within a specified range, perform one of the following operations listed above and click the Negate checkbox.
4. When you are satisfied with the values you have enter, click Ok.

Working with Ranges of Elapsed Seconds

You can specify a range when filtering for log entries that only meet the criteria for the number of seconds that have elapsed since the log was received by the Log Viewer.

To specify a range using the destination or source port number as a criteria:

1. Right-click either the Src Port or Dst Port column. Security Manager displays either the Filter for Bytes In or Filter for Bytes Out dialog box.
2. To display only log entries that contain a source or destination port number that is within a range of values, perform one of the following steps.
   - To filter on a minimum port number value, click in the From checkbox, click the From value list box and select a value.
   - To filter on a maximum port number value, click in the To checkbox, click the To value list box and select a value.
   - To filter on both maximum and minimum port number values, select both To and From, then click the appropriate list box and select a value.
3. To display only log entries that do not contain a source or destination port number value that is within a specified range, perform one of the following operations listed above and click the Negate checkbox.
4. When you are satisfied with the values you have enter, click Ok.
Using Log Views

When you use filters, you create a unique, customized view of your log entries. You can save this view (with all its filters) so you can use it again. Use the pre-filtered views to see critical severity attacks, configuration log entries, scans, etc.

For example, you might want to create views to help you 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. Filter on the device vin column.

You can also hide (and unhide) log entries to display specific information.

Saving Views

If a specific view of the Log Viewer contains a lot of important information, you can save the view. Important data in a given view might include filters you created for specific source and destination pairs and specific log entries that display in a specific view. You can retrieve the view later to view it. You can also apply filters associated with this view and apply it to another instance, avoiding creating an elaborate filter.

To save a view of the Log Viewer, click the File menu and click the Save As option. Security Manager displays the Save As dialog box. Type a string in the Enter View Name field that you want to be the name of the saved view of the Log Viewer and click Ok. You have now saved the view. To return to the view after logging off from Security Manager, simply log in again and Security Manager displays the view.

Exporting Views

If you want to save a specific view to a specific format, you can export the view to either an Adobe PDF file or a standard PostScript file. This can be helpful for later viewing and for transferring a view file between administrators. To export a view:

1. In the menu bar, Click the File menu and select Export to PDF or Export to PostScript. Security Manager displays the export dialog box.
2. Browse to the directory where you want to save the view.
3. Enter a filename in the File Name box (ensure that the file extension is set to PDF or PostScript).
4. Click Export to export the view to a file in the format you specified.
Customizing Columns

You can configure the Log Viewer to include varying levels of data associated with setting types in the Log Viewer’s columns. Column settings refer to the value types that appear along the Top Axis of the Log Viewer. As a means of limiting or expanding the amount of data that is available to you in the Log Viewer, you can configure the Log Viewer to display as many potential columns as you want. The Log Viewer provides up to 40 column settings from which you can choose. If you set too many columns, you may have to use the scroll bar to move from side to side of the extremities of the Log Viewer to view all columns. The default number of columns is 16.

In selecting columns to display in the Log Viewer, you need to determine whether you want more or less information. Generally, you may want to display fewer columns in the following instances:

- You have enough detail about much of the activity you are viewing.
- You are only interested in certain types of data

You can also reorder columns.

Example: Customizing Columns

You may be interested in only the following information:

- The types of attacks are entering your site.
- The specific devices that are generating the attacks.
- The date and time of the attacks.

For these instances, you would simply specify that the Log Viewer display data only for the Time Received, Attack, and Source Address columns. Also, you may value some information more than other types and you may want to arrange it closer to the left side of the Log Viewer. For example, you may be more interested in seeing a source address before you see information about attacks so you may want to move the source address column closer to the time received information at the left of the Log Viewer. To configure the Log Viewer to accept only these columns:

1. Click the Log Viewer option in the Navigation Tree to display the Log Viewer.
2. Click the Choose Columns button or click the column header and drag the column to the right or left. Security Manager displays the Column Settings dialog box.

**Note:** The Column Settings dialog box contains a list of all column headings that appear in the Log Viewer. A checkbox accompanies each entry; the first 16 checkboxes are checked indicating that these strings display as default column headings in the Log Viewer. The checkboxes occur as toggled items.
3. Click all of the checkboxes to remove checks from them except for the columns you want to see:
   - Time received
   - Attack
   - Source address

4. To move the Source Address column further to the left to be adjacent to the Time Received column, click the source address string to highlight it (make sure the checkbox stays checked) and click the Move Up button. Security Manager positions the source address string above the attack string just below the time received column.

5. Click Ok. Security Manager displays the Log Viewer again, this time with only the three columns of information you specified as the following figure shows.
To hide and move columns:

- To display selected columns, click Show.
- To hide selected columns, click Hide.
- To reorder the columns, use Move Up and Move Down.
- To change the width of the columns, select the column extremity line and drag to the right or to the left.
- To close the Log Viewer, click Ok.

**Fine-Tuning with the Log Viewer**

Fine-tuning your system is a step-by-step iterative process. Typically, you begin fine-tuning by examining your log entries through the Log Viewer, Report Manager, or the Log Investigator, then making changes to your device configuration, firewall or VPN policy, or your logging settings. When new log entries appear that reflect those changes, you again examine the log entries to see the results.

In Security Manager, all the modules (Log Viewer, Policy Manager, etc.) work together to help you explore and respond to network activity.

**Jump to Policy**

To quickly edit a firewall or VPN rule in a policy from the Log Viewer, double-click a policy in the Policy column. Security Manager displays the policy with the firewall or VPN rule that generated the log entry.

**Identify Irrelevant Attacks**

Irrelevant attacks are events that do not affect your network or that you do not consider important. You identify irrelevant attacks because:

- You can reduce the number of log entries and increase system performance.
- You can isolate log entries for harmless attacks.
- You can 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:
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>
<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>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>

If the attack is irrelevant, you can remove the matching Attack Object from the rule that triggered the log, or monitor the Attack Object using custom severity setting.

**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. Security Manager displays the device configuration for the device, enabling you to make changes to the device.
Chapter 11 Logging

USING THE LOG INVESTIGATOR

The Log Investigator provides a cross-tabulation of the most common pairs of the following entities seen by the NetScreen FW/VPN device: destination, source, attack, and port. The Log Investigator can help you determine the following information:

- The number of log entries on the network that are indicating of a pattern.
- Which systems are being attacked the most.
- What services are being attacked the most.
- Which sources are common attackers.

The regions of Log Investigator are shown in the following illustration.
Using the Log Investigator

The following table details the various regions in the Log Investigator.

<table>
<thead>
<tr>
<th>Region</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Display</td>
<td>A region that displays the types of categories and time received detail for filters used for the Log Investigator.</td>
</tr>
<tr>
<td>Number of Logs Selected</td>
<td>A value that indicates the number of log entries selected to be evaluated by the Log Investigator.</td>
</tr>
<tr>
<td>Left Axis</td>
<td>A list of entities within a prescribed entity type for which the Log Investigator establishes a ranking first before performing a ranking on the entities in the Top Axis. Also known as the independent axis.</td>
</tr>
<tr>
<td>Top Axis</td>
<td>A list of entities within a prescribed entity type for which the Log Investigator establishes a ranking after performing a ranking on the entities in the Left Axis. Also known as the dependent axis.</td>
</tr>
<tr>
<td>Zoom In Detail</td>
<td>Displays a textual list of a ranking of top system ports, attack types, or times associated with a given pair of entities in the Log Investigator.</td>
</tr>
<tr>
<td>Zoom In Chart</td>
<td>Displays a list in chart form (either bar or pie chart) of a ranking of top system ports, attack types, or times associated with a given pair of entities in the Log Investigator.</td>
</tr>
</tbody>
</table>

Security Manager can potentially generate a very large number of log entries. The Log Investigator enables you to explore the data in the log entries in the following ways:

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

Using the Log Investigator, you can analyze a large volume of log entries to obtain information where the most concern lies. The ability to analyze this data decreases your risk and increases security. You can view summary information and determine what network activity is expected and the severity level of the activity. Also, you can also correlate log entries to focus on activity that poses a risk to your network.

You can correlate the following criteria in the log data based on sampling from a specified time period:

- Top Sources
- Top Destinations
- Top Attacks
- Top Destination Ports

By right-clicking on various levels of data, you can zoom into the highlighted portion of the Log Investigator.
Chapter 11 Logging

Working with Log Investigator Data

The following example uses the data displayed in the initial figure of the Log Investigator. View the cell defined by column head with the destination address 63.172.115.6 and row head with the source address 63.172.115.190. Note that Log Investigator displays 140 log entries for this location pair.

This high value might indicate that a high number of significant events are occurring between these two nodes. Potentially, the source device (63.172.115.190) is sending a high number of attacks to the destination device (63.172.115.6).

To view more detail on this activity, right-click the cell and click the Zoom In option and then click the Dst Port option. Now you can view how many records are associated with specific ports on the device.

The following figure displays two areas in the bottom portion of the Log Investigator which provides more detailed information on the selected log after selecting the Zoom-In option on a cell. Both regions enable you to view the number of log entries associated with each system port on the device. The right region displays in chart form the same information as the left region displays, in this example, a Bar Chart. Both regions list ports in the descending order by log count with the port with the highest number of log entries associated with it displayed above all others, the port with the second highest number of log entries displayed below the top one, and so forth.

By viewing the port with the most common attacks, you can determine what type of service the attacker is targeting.
You can also right-click the cell and select the Attacks option from the Zoom In option to display a narrative view of attack information displayed on the left and a chart view of the information in the lower right.

Note that the lower left region displays that the TCP C25-OLDPACKET:OLD-ESTB is the most common attack in the attack list with 130 instances of it entering the device.

You can also view log entries by a time range, identifying what times experienced the most log entries. To view log counts by time intervals, right-click the cell you want to examine, click Zoom In and click the Time option. Security Manager displays Time Zoom In areas as shown in the following figure.
After reviewing this information, you may decide you want to exclude an item to see if less records are generated when the item is removed. To exclude an item, right-click a cell and click the Exclude option. This removes the cell from consideration. Now you can check to see if the same types of log entries are generated. The excluded cell now appears in the Configuration display area along with the types of filters applied and the types of attacks for which you are scoping.

**Configuring the Log Investigator**

To configure the Log Investigator:

1. Create a filter and apply it to a set of log entries. Filters specify both the columns and log categories you want to display.
2. Run the Log Investigator to create a ranking of data points based on the Left Axis or Independent Axis.
3. In the Log Investigator Options dialog box, specify the top 10 data points on the Left Axis. The data in the Left Axis is the data in which you are most interested.
4. In the Log Investigator Options dialog box, specify the duration to be one day.

**Setting the Number of Data Points on Each Axis**

The default number of entity pairs being evaluated for activity between them is 10 for each (a matrix of 100 cells). However, you can alter this value for both axes. The Left Axis, by default, contains the Top Sources list is considered the independent axis because it is the control or the first data set in the matrix.

To change the number of Left Axis locations being evaluated, type a desired value in the Data Point Count box under the Left Axis region. The Top Axis, by default, contains the Top Destinations list is considered the dependent axis because it occurs second. To change the number of Top Axis locations being evaluated, type a desired value in the Data Point Count box under the Top Axis region.

For example, assume the Log Investigator filter is set to Attacks. If you select as the independent axis Top Sources, and then select Top Destinations for the dependent axis, the table displays all attacks by source along the independent axis. The dependent axis displays the number of attacks for each of the top destinations according to that source.

If you were to change the axes, with Top Destinations as the independent axis and Top Sources as the dependent axes, the table then displays all attacks for the top destinations with the dependent axis displaying the number of attacks for each source by destination. This set of data is not the same as the first example.

**Selecting Data**

The Log Investigator enables you to select data in two ways:

- By selecting individual cells of data
- By selecting multiple columns of data
Selecting By Individual Cells

By selecting a cell for the Log Investigator to analyze, you are essentially isolating only one location pair. You are evaluating all transmissions that have occurred during a time period between one specific source and either one specific destination, a port or an attack and a destination port.

This approach can be useful after you have identified one entity in the location pair as being involved in suspicious activity.

For example, after some review of activities across multiple destinations, your network performance has slowed and you believe that one location pair is creating a bottleneck effect in the network by exchanging too much data. You may see that one source location, for example, 192.179.20.3 is sending an unusually large number of transmissions to source location 192.179.16.27.

This activity could be batch files being auto-archived at a high-peak hour or even an employee archiving many large files (perhaps radiology photographs in a hospital) at a certain time every day before leaving for home. This activity may be creating the bottleneck. For this type of anomaly, the examination by cell may be a useful way to use the Log Investigator.

Selecting Axes

By selecting a column head in the Log Investigator for analysis, you are essentially identifying all available entities involved with other entities, for example all available sources sending attacks to one destination. For example, you may have sources 192.179.12.20, 192.179.12.29, and 192.179.12.41 showing up in the Source column in the Log Investigator. By selecting the column head for destination 192.179.23.6, you are obtaining data of all source transmissions to the one destination. A sample column selection that displays all available source transmissions to one destination is shown in the following figure.
This approach can be useful in analyzing collective data from multiple sources by one destination.

For example, you might have one destination 192.179.23.6 receiving a large amount of data from many sources 192.179.12.20, 192.179.12.29, and 192.179.12.41 that is slowing the network. Perhaps multiple users are attempting to contact only one application server at the same time when it might be possible to distribute exchanges between users and multiple servers.

By selecting a column for examination in the Log Investigator, you can view this environment more meaningfully. You can obtain a more detailed view of what is happening at one destination to determine why performance has degraded.

### Benefits/Limitations of Different Analysis Levels

The following table details the benefits of each type of Log Investigator analysis.

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Benefit</th>
</tr>
</thead>
</table>
| Multiple | Multiple    | • Provides a wider view of activity on multiple destinations and multiple sources. Gives you access to many location pairs, enabling the viewer to make decisions about which specific pairs to examine individually.  
  • Provides the broadest possible view of network activity. |
| Multiple | One         | • Provides a wider view of activity on one destination and may yield data that indicates why the performance has degraded on that destination. |
| One      | Multiple    | • Provides a wider view of activity on one source and may yield data that indicates why a source has sent attacks to multiple destinations. |
| One      | One         | • Provides a succinct view of one location pair enabling you to zero on a specific activity.  
  • Requires little processing power and does not degrade network performance.  
  • Does not distract the viewer with too much data. |
Setting Log Investigator Parameters

While the activity that the Log Investigator generates data for are set in Security Manager by default, you can still control some aspects of the data reporting process in the Log Investigator. You perform these steps by clicking on the Set Log Investigator Options button that launches the Log Investigator Options dialog box.

You can set the following parameters to configure the data that the Log Investigator examines.

Configuring a Time Interval

You can configure a time period in which you want the Log Investigator to display data for activity between location pairs for examination. You configure the time interval in the Time Period region in the Log Investigator Options dialog box by specifying the interval type (either weeks, days, hours, minutes, or seconds) and then selecting the number of the interval type in the Duration field. Note that you can only configure a past time period. For example, if you want to find all the attacks that occurred during the past week or several hours that arrived at a specified IP address, you would indicate the time during which you believed the attacks occurred.

If you want a broader trending of the activity between top sources and destinations, you may want a longer interval. If you want a more random sampling of the activity, you can specify a shorter interval. The shorter interval provides you with the advantage of giving you easy access to data without having to analyze too much of the overhead associated with a longer interval. Also, if you have a specific period in which you feel the data is significant, the shorter interval can be more helpful in locating the suspicious activity.

Configuring a Beginning Time

You can specify the time when the snapshot of the location pair activity begins. You can specify the snapshot beginning point in two ways:

- Using the current time as the beginning point
- Using a specified time as the beginning point
The default setting for this parameter is Most Recent that indicates that the evaluation of the event’s trend begins with the most current access to the monitoring of the system (the current date and time). This approach is useful when you are either randomly troubleshooting for recurring activity or if you anticipate your network behavior will begin to alter because of known external influences that are expected to occur.

You can also specify a more customized beginning point for event evaluation by selecting Starting At and providing a specific time. The time you specify indicates when the event tracking begins. This approach is useful when you know of events that have occurred during a given time period or began occurring at a specific time, and you want to see data on the event during this period.

### Setting the Data Type

You can also change the data type that the Log Investigator will analyze for each of the axes. You can change the data type to one of the following data types described in the following table.

<table>
<thead>
<tr>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>The IP address that sends the attack</td>
</tr>
<tr>
<td>Destination</td>
<td>The IP address that receives the attack</td>
</tr>
<tr>
<td>Attacks</td>
<td>The attack type</td>
</tr>
<tr>
<td>Destination Ports</td>
<td>A port number that indicates a specific service type</td>
</tr>
</tbody>
</table>

To set the data type for log investigation in a given axis (either Left Axis or Top Axis), click the Data Point Source list box in either axis and select a data type.

### Setting a Log Entry Limit

The data you see in the Log Investigator is obtained from a log buffer created from data generated from the Device Server. The Log Investigator only obtains selected data (two fields) from this buffer that it places in the matrix you see in the GUI. The buffer can quickly fill up with log entries because of the variety of log entries that can be generated for many types of activities that Security Manager monitors.

If the buffer becomes too large, the Log Investigator may have difficulty placing information in the matrix and performance can degrade. The buffer can expand to one million log entries, although at that size, it will use memory on the server.

You can set a lower limit on how large the log buffer can expand to before it stops accepting log entries by clicking on the Max. Log Count list box in the Additional Query Constraints region. The lowest limit for the size of the log buffer is 100,000 entries.
Using the Log Investigator

Zooming on Data

The Log Investigator lets you to analyze data in a number of ways to obtain a more meaningful understanding of activity between a source and destination location. After you have established the top location pairs, you can then begin to examine the data more closely. To begin closer examination:

1. Right-click a cell or a column for which you want more data. Security Manager displays the Log Investigator popup configuration menu.
2. Click the Zoom In option in the Log Investigator popup menu. Security Manager displays a submenu.
3. Click the Dst Port option. Security Manager populates two areas in the Log Detail region at the bottom portion of the Log Investigator with data.

You can view the log associated with a specific entity in the Log Viewer. To view in the Log Viewer the log of the entity displayed in the Log Investigator:

1. Right-click a cell that you want to view in the Log Viewer. Security Manager displays the Log Investigator popup configuration menu.
2. Click the View in Log Viewer option. Security Manager displays the Log Viewer, showing the log related to the entity in the Log Investigator.

About Zoom In Data

Take a few moments to review the two areas in the Log Detail region. They are:

- The Zoom In text area on the left side.
- The Zoom In chart area on the right side.

The Drill Down Data area breaks the data down of the destinations into port numbers listing in the left column the actual port number and in the right column the number of attacks received by the port number. This information is helpful because specific services are mapped to a port number. By identifying the service that is being attacked, you can determine valuable information about the behavior and type of the attack.
Log Investigator Example

The following example details a scenario where you would use the Log Investigator to examine pairs of sources and destinations.

<table>
<thead>
<tr>
<th>Company Type/Node Distribution</th>
<th>NetScreen Hardware</th>
<th>Event Attributes</th>
<th>Filtering Strategy</th>
</tr>
</thead>
</table>
| Private services company working with county government | NetScreen-500 in the central office with each branch office containing several NetScreen-5XTs. | • HTTP Service  
  • Port 80  
  • Specified times of day  
  • Specified dates | Designating a dedicated NetScreen-5XT in each branch office to accept only log source and destination information that meet time and attack type requirements. |

This organization is divided into one central site and several regional sites. The central county office then works with regional county sites. Recently, to fulfill federal regulations, the organization began a tracking program where outside people involved with the organization are required to fill out an internet form that breaks down the types of materials they are using.

When an applicant has reached a limit of a certain material they are using, they can no longer work with the county. Recently, an attacker sent multiple forms from various fictitious names, appending each with an attack to corrupt existing database records to bypass the material limits. The attacks arrive early in the morning before the main network administrators arrive at work.

To obtain more information about the attacks that occurred, specifically source IP address information and port number information that would indicate the HTTP service, the network administrators have configured a designated NetScreen-5XT at each of the regional county landfill offices cluster offices that specifically attempt to display top sources, top destinations, and breaking attacks down by port number. Specifically, they configure the Log Investigator to examine data that meets only the following conditions:

- Attacks that arrive between 4 and 8 a.m.
- Attacks that occur between April 7 and 21 on the weekdays.
- Attacks that arrive on Port 80 which is associated with the HTTP service.

To configure the Log Investigator to display only event types that have occurred recently that fulfill these conditions:

1. Click the Log Investigator option in the Navigation Tree to display the Log Investigator.
2. Click the Set Log Investigator Option button in the button bar. Security Manager displays the Log Investigator Options dialog box.
3. In the Time Period, type the value 4 in the Duration box and click the Duration list box and select hours to configure the logging to occur for four hours.
4. In the toggled radio button pair under the Duration region, click the Starting At radio button and click the following fields in the time list box and make the following changes using the Up and Down arrows to the right of the list box:
   - Click the hours fields and change it to 04.
   - Make sure that both the minutes and the seconds fields display 00. If they do not, use the arrows to change them to 00.
   - Click the AM/PM field and change it to AM. The time should now read 04:00:00 AM.

5. Make sure the selection in the Datapoint Source list box in the Left Axis region is Top Sources and that the Data Point Count value is 20.

6. Make sure the selection in the Datapoint Source list box in the Top Axis region is Top Destinations and that the Data Point Count value is 20.

7. Click Ok.

You may see some significant cells displayed. For these cells, you may want to see more detail. To examine more detail for each, right-click the cell, then click the Zoom In option and then click the Dst Port. The Log Investigator displays a list of most common system ports associated with each of the log entries. Review the list to see if the list contains Port 80. If you see a significant amount of activity in Port 80, you may have a good candidate to identify the intruder.

**Excluding Log Investigator Data**

In addition to automatically generating only certain types of data for the Log Investigator, you can also choose to manually remove entire rows and columns of data received by the Log Investigator. This can be useful in removing values that are not of interest or to allow showing more lower-ranked values on either axis. For example, in a display where you have the top 20 instances, you exclude 10. The Log Investigator displays instances 21 through 30. This technique of removing entire rows or columns is known as excluding.

To exclude a row or a column:

1. In the Navigation Tree, select Log Investigator.
2. Click a row or column header to highlight the entire row or column.
3. Right-click the highlighted row or column. Security Manager displays a configuration popup menu.
4. Click the Exclude option.
Security Manager removes the column or row and indicates the removed column or row in the top portion of the Log Investigator as shown in the following figure.

**Setting Filters for Log Investigator Data**

The Log Investigator enables you to specify a condition that represents one of the values displayed in the Log Viewer to test when data is being sent. You can test any parameter that is represented in the columns of the Log Viewer. To test this condition, you need to create a special condition object known in Security Manager as a filter. A filter contains two types of data:

- The actual data type that the Log Investigator tests
- A value assigned to the data type

Typical filters are timestamp filters, for example, time received or time generated or packet directional filters, for example, inbound if or outbound if. Note that filters in the Log Investigator are configured and act the same way as they do in the Log Viewer. The following table details filter types:

<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, Time Generated</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>Address Filter</td>
<td>Source Address, Destination 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>
</tbody>
</table>
To configure a filter:

1. In the Navigation Tree, select Log Investigator.
2. Click the Log Investigator Set Filter button.

Security Manager displays the Filter Summary dialog box.

3. Click a column name listed in the left pane on which you want to apply a filter.
4. Click either the From or To checkbox and select a timestamp filter that you want to apply to column on which you are filtering.
5. Click Ok. The Log Investigator now displays only data that meets the filter you created in the column you specified.
The Audit Log Viewer monitors events that occur when a Security Manager administrator has changed an object setting on the system. This feature enables you to track what changes were made to your environment. You can track changes by time of logging. You can access audit log entries to see all data for your domains, one domain at a time. In addition, you can view details of the change to the object in the appropriate configuration environment. The following table describes the columns of information presented in the Audit Log Viewer.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Received</td>
<td>Displays the time the object was changed.</td>
</tr>
<tr>
<td>Admin Name/Domain</td>
<td>Displays the name of the user who changed the object or the name of the domain in which the changed object resided. The domain can be either the Global Domain or a user-created domain.</td>
</tr>
<tr>
<td>Action</td>
<td>Displays the type of change applied to the object.</td>
</tr>
<tr>
<td>Object Type</td>
<td>Displays the type of object that was changed.</td>
</tr>
<tr>
<td>Object Name</td>
<td>Displays the name of the object which underwent the change.</td>
</tr>
<tr>
<td>Log ID</td>
<td>Displays an assigned log ID number.</td>
</tr>
</tbody>
</table>

The following figure shows a sample view of the Audit Log Viewer.
The Audit Log Viewer contains two types of objects that include detailed views:

- A target which is a directive you perform on a device.
- The device itself.

You can double-click a target that appears in the Targets column to display target detail in the Target List lower left box in the Audit Log Viewer. You can double-click a device that appears in the Devices column to display device change detail in the Device List in the lower right box in the Audit Log Viewer.

By double-clicking on an entry in either the Targets or Devices detail box, Security Manager displays a dialog box where a change occurred within a specified time period. The change is indicated by a solid green triangle.

Targets can be found in various portions of Security Manager including VPN Manager, Device Manager, and the Object Manager.

The Audit Log Viewer displays log entries in order of time generated by Greenwich Mean Time (GMT). You can also control what the current log is by a time value. By configuring a time value in the log entries are displayed by a time value. Click the View Menu and select the Go To Log By Time option. Security Manager displays the Log By Time dialog box. By selecting a date and time, the Audit Log Viewer now displays all log entries beginning from the date and time you specified.

**Configuration Administration Settings**

After you have entered the Audit Log Viewer, you may want to change your configuration. To configure an administrative change, double-click a target in the target list of the Target Detail region in the lower left hand portion of the Audit Log Viewer screen. Security Manager displays the Admin > General dialog box.

You can set an administrative owner of the target you selected by typing a name in the name fields and providing primary and secondary Email addresses, and primary and secondary phone numbers. You can also code the target with a color in the Color list box.

You can also set authorization for the target owner by clicking on the Authorization Tab and clicking on the Local Password field and typing a string that will be the password for the owner to have access to the target. You can also provide permissions level to the target owner by clicking on the Permissions Tab and clicking on the System Administrator field and typing a role setting and domain name.

The Audit Log records several types of actions:

- SYS_LOGIN
- SYS_LOGOUT
- DB_INSERT
- DB_UPDATE
- DB_DELETE
- DEVICE_REBOOT
- EXEC_SOFTWARE_KEY
- UPDATE_CONFIGURATION
- UPGRADE_FIRMWARE
- DOWNLOAD_RUNNING_CONFIG
- GENERATE_CERTIFICATE_REQUEST
- UPLOAD_FULFILLED_CERTIFICATE
- DELETE_CERTIFICATE
- FLASH_SYNC
- SET_ROOT_ADMIN
- DEVICE_FAILOVER_REVERT
In This Chapter:

- About Reporting
- Report Types
- Setting Report Options
- Log Viewer Integration
- Using Reports
- Using Historical Reports

Use the Report Manager module in Security Manager to generate and view reports summarizing log and alarm originating from the managed FW/VPN devices in your network. You can use these reports to track and analyze log incidents, network traffic and potential attacks.
ABOUT REPORTING

The Report Manager module in 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 FW/VPN devices in your network. The reports in Report Manager provide a useful complement to the monitoring and logging capabilities in 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. There are four groups of reports:

- **FW/VPN.** Series of six reports summarizing log and alarm data generated by the managed FW/VPN devices in your network.
- **DI.** Includes eight reports that provide data on deep inspection attacks.
- **Screen.** Includes five reports that provide data on Screen attacks detected by the firmware on the managed FW/VPN devices in your network.
- **Administrative.** Includes two reports specifically designed to help system administrators track and manage log incidents and security rules.

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. Refer to “Report Types” on page 439 for more information on each of the specific reports per group.

For details on each report type grouping, refer to the online help.
Graphical Data Representation

Report Manager presents the data in each report in both tabular and graphical form. The various depictions of the data make it easier to identify trends. Depending on your preference, you can view the data in either a horizontal bar graph or a pie chart.
Integration with Logs

Report Manager is also integrated with the Log Viewer and Log Investigator modules. By simply clicking on 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 442 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

There are 21 pre-defined reports in the Report Manager module. Each report provides a summary of key log events and alarms generated by the FW/VPN devices managed in your network.

For your convenience, Report Manager group reports into the following four categories:

- FW/VPN Reports
- DI Reports
- Screen Reports
- Administrative Reports

FW/VPN Reports

The following table lists and describes reports in Security Manager that provide information related to your network’s firewalls and VPNs.

<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 FW/VPN 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 FW/VPN devices in your network.</td>
</tr>
<tr>
<td>Top Traffic Log</td>
<td>the total number of traffic log entries generated by the managed FW/VPN 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 FW/VPN 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 FW/VPN 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 FW/VPN devices in your network, within filter constraints.</td>
</tr>
</tbody>
</table>

DI Reports

The following table lists and describes reports in Security Manager that provide deep inspection information.

<table>
<thead>
<tr>
<th>Report</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Attacks</td>
<td>which attacks are most frequent.</td>
</tr>
<tr>
<td>Attacks by Severity</td>
<td>the number of attacks by severity level (set in attack objects).</td>
</tr>
<tr>
<td>Attacks over Time</td>
<td>a summary of when deep inspection attacks occur on your network.</td>
</tr>
<tr>
<td>Top Attackers</td>
<td>where attacks originate from most frequently.</td>
</tr>
</tbody>
</table>
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.

### 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>
<thead>
<tr>
<th>Report</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Attacks</td>
<td>the most common attacks detected by the firmware on your FW/VPN device.</td>
</tr>
<tr>
<td>Attacks by Severity</td>
<td>the number of attacks detected by the firmware on your FW/VPN device</td>
</tr>
<tr>
<td>Attacks over Time</td>
<td>a summary of when attacks are detected by the firmware on your FW/VPN device</td>
</tr>
<tr>
<td>Top Attackers</td>
<td>where attacks originate from most frequently.</td>
</tr>
<tr>
<td>Top Targets</td>
<td>which hosts on your network are the most frequent targets of attackers for firewall attacks.</td>
</tr>
</tbody>
</table>

### Administrative Reports

The following table lists and describes reports in Security Manager that provide information specifically for administrators:

<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 online help.
**Setting Report Options**

Each report in 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 on the chart on each report.

For more specific information describing how to configure reports options, refer to the online help.

### 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 (i.e., 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.
Chapter 12 Reporting

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.

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 on a data point in any report and select Log Viewer from the View menu. The source log entries will appear in the Log Viewer.
Using Reports

The following examples describe typical use cases for the reports in 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 predefined 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.
In this example, you are a security administrator responsible for implementing new rules to your firewall rulebase. Once you have updated the new security policy on the managed FW/VPN 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.
Using Reports

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 FW/VPN 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 FW/VPN devices.
Example: Using Screen Reports to Identify Attack Trends

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 that there has been a recent increase in attacks as detected by your firewall. You can then 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 online help.

Example: Using Deep Inspection 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 online help.
Chapter 12 Reporting

**Using Historical Reports**

If you previously used Historical Reports in NetScreen-Global PRO, you can continue to do so as part of your Security Manager implementation.

Refer to the NetScreen-Security Manager 2004 Installer’s and Migration Guide for more information on maintaining your previous implementation of historical reporting with 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.
**Glossary**

**Action (Deep Inspection).** A DI action is performed by a NetScreen FW/VPN device when the permitted traffic matches the attack object specified in the rule. Deep Inspection actions include drop connection, drop packet, close client, etc.

**Action (firewall).** An firewall action is performed by a NetScreen FW/VPN device when the device receives traffic that matches the direction, source, destination, and service. Firewall actions include permit or deny.

**Activate Device wizard.** The Activate Device wizard guides you through activating a modeled device in the Security Manager User Interface.

**Add Device wizard.** The Add Device wizard guides you through importing or modeling a new device to the 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 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 NetScreen FW/VPN device to check its own route table. If the IP address is not in the route table, the NetScreen FW/VPN device denies the traffic.

**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.

**Atomic Configuration.** Atomic configuration is a fail-safe feature in ScreenOS 5.0. For devices running ScreenOS 5.0, 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 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 NetScreen FW/VPN devices to detect known attacks and prevent malicious traffic from entering your network.

**Attack Protection.** Attack Protection is defined by the attack objects, protection options, attack severity, and alerts.

**Audit Log Target.** An Audit Log Target is a directive that was sent to a NetScreen FW/VPN device.

**Audit Log Viewer.** The Audit Log Viewer is a module of the Security Manager User Interface. The Audit Log Viewer records administrative actions. Each audit log includes the date and time the administrative action occurred, the 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 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.

**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.

**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.

**CLI.** The CLI is the command line interface.

**Configlet.** A configlet is a small, static configuration file that contains information on how a NetScreen FW/VPN device can connect to NetScreen-Security Manager 2004.

**CRC Errors.** CRC errors indicate the number of packets generating a cyclic redundancy code error processed through the NetScreen FW/VPN 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.

**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 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.

**Demo Mode.** Demo mode is a demo version of the Security Manager User Interface that does not connect to a Security Manager management system. Although demo mode uses dummy data, it contains similar functionality as the production version of Security Manager UI.

**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 NetScreen FW/VPN 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 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 Security Manager to your managed devices. Directives include importing, updating, rebooting, etc. When you send a command to a device or group of devices, 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. DDoS attacks This 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.

**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.

**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.
**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 Policies.** A firewall policy defines access to your network, including allowed services, users, and time periods. Use firewall policies to control the shape of your network traffic as it passes through the firewall, or log specific network events.

**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.

**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.

**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 Security Manager operations on multiple FW/VPN devices at the same time.

**GUI Server.** The GUI Server manages the system resources and data that drives Security Manager functionality. The GUI Server contains the Security Manager databases, and centralizes information for devices, their configurations, attack and server objects, and policies.

**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 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.

**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.

**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 Security Manager UI.

**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, 128.11.2.30. 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 NetScreen FW/VPN device flags the event as an IP sweep attack and drops the connection to prevent replies.

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 Security Manager User Interface. Job Manager tracks the progress of the command as it travels to the device and back to the management server.

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 NetScreen FW/VPN 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.

Load Balancing. Load balancing distributes workload to processors to improve the throughput of a concurrent connections.

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, etc.).

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 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 Security Manager User Interface. The Log Viewer displays log entries that your NetScreen firewalls generate based on criteria that you defined in your firewall 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.

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.

Management System. The Management System is the Windows or Solaris server that a GUI Server and Device Server is installed on.

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.

Menu bar. The menu bar is the upper section of the Security Manager UI. The menu bar contains accessible commands.

Modeling. Modeling is the process of creating a non-deployed device configuration in the Security Manager UI.

Modules. A module is a first-level element in the Security Manager navigation tree.

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 firewall policies and VPNs; when you update a device, that device automatically replaces the global NAT object with its device-specific NAT configuration.

Navigation Tree. The navigation tree displays the 11 Security Manager modules in the left pane of the Security Manager window.

NetScreen FW/VPN Device. A NetScreen FW/VPN is a NetScreen-produced device that you use to enable access to your network components and to protect your network against malicious traffic. NetScreen Security Manager can manage NetScreen FW/VPN devices running ScreenOS 5.0 and ScreenOS 4.0.x (except 4.0.2). All devices from NS-5XT to the NS-5400 are supported, except the NS-5, NS-10, and NS-1000. Security Manager also supports the NS-5GT running ScreenOS 4.0-DIAL2. Security Manager can also manage vsys configurations, NSRP clusters, and extranet devices.

NetScreen Redundancy Protocol (NSRP). NSRP is a proprietary protocol that provides configuration and run time object (RTO) redundancy and a device failover mechanism for NetScreen FW/VPN devices in a high availability (HA) cluster.
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.

Object Manager. The Object Manager is a module of the Security Manager User Interface. The Object Manager contains the Objects used in your Security Manager system. An object is a reusable, basic 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 Security Manager, objects are shared objects, meaning they are shared between the global domain and all subdomains. Objects are the building blocks of the Security Manager management system.

On-Site Admin. The on-site admin is the person who installs a configlet using Rapid Deployment.

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).

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 NetScreen FW/VPN device to detect and reject oversized or irregular packet sizes.

Policy Manager. The Policy Manager is a module of the Security Manager User Interface. You can use Policy Manager to configure firewall and VPN policies for your managed devices.

Policy. A firewall policy is the combination of both firewall rulebases and all rules into a comprehensive plan that defines how the NetScreen FW/VPN device works on your network.

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 NetScreen FW/VPN device flags this as a port scan attack and drops the connection.

Process Status. The process status displays information about processes on a NetScreen FW/VPN device.

Protocol. Protocols are predefined services (HTTP, SNMP, Telnet, etc.) that are enabled for the NetScreen FW/VPN device.

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 NetScreen FW/VPN devices. Typically, you use a VPN to enable RAS, then add RAS users to the VPN.

Realtime Monitor. The Realtime Monitor is a module of 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.

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 Security Manager User Interface. Use Report Manager to generate and view reports summarizing log and alarm originating from the managed FW/VPN 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 Redistribution.** Router redistribution is the exporting of route rules from one virtual router to another.

**Rule.** A rule is a statement that defines a specific type of network traffic. When traffic passes through the FW/VPN 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.

**Rulebase.** A rulebase contains rules. a rulebase provides a method of detecting and acting upon suspicious traffic. In Security Manager, there are two firewall policy rulebases: zone-specific and global.

**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 Server Protocol (SSP).** For communication between the UI, the GUI Server, and the Device Server, 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.

**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 Manager administrator.** The Security Manager admin is the person who uses Security Manager User Interface to manage their FW/VPN devices.

**Security Parameters Index (SPI).** The SPI is a hexadecimal value which uniquely identifies each tunnel. It also tells the NetScreen FW/VPN device which key to use to decrypt packets.

**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 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 Security Manager system.

**Service Object.** Service objects represent the IP traffic types for existing protocol standards. NetScreen FW/VPN devices monitor and manage network traffic using these protocols. 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.

**SHA-1.** Secure Hash Algorithm-1, an algorithm that produces a 160-bit hash from a message of arbitrary length. SHA-1 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.
**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 NetScreen network security devices are stateful inspectors.

**Status Bar.** The status bar is the lower section of the Security Manager UI. The status bar displays supplemental information.

**Subdomain.** A subdomain is a domain 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 allows 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 Administrator.** 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.

**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 NetScreen FW/VPN device sees this discrepancy in a fragmented packet, it drops the packet.

**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.

**Toolbar.** The toolbar is the upper section of the Security Manager UI. The toolbar contains icons that relate to accessible commands.

**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 allows computers with different operating systems to communicate with each other. 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.

**Tunnel Interface.** A tunnel interface 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.

**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 NetScreen FW/VPN 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.

**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 Security Manager graphical User Interface (UI) is used to control the Security Manager system. Using the UI, you can configure Security Manager administrators, add devices, edit policies, view reports, etc.

**User Object.** User objects represent the users of your managed devices. You can include user objects or groups in firewall policies or VPNs to permit or deny access to individuals or groups.

**User.** A user is a person using the network your NetScreen FW/VPN devices are protecting. Security Manager support 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 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 NetScreen FW/VPN device supports 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 NetScreen FW/VPN 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 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.

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 NetScreen FW/VPN 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.

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).
NetScreen-Security Manager 2004

Unmanaged Commands

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 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 Security Manager may support these commands). To use an unmanaged device command, you must connect locally to the NetScreen FW/VPN device.

The table below details each unmanaged command:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>These commands configure or display administrative parameters for NetScreen FW/VPN devices, such as:</td>
</tr>
<tr>
<td></td>
<td>• Characteristics for each admin user, such as password and privilege level</td>
</tr>
<tr>
<td></td>
<td>• How the device performs admin user authentication</td>
</tr>
<tr>
<td></td>
<td>• Ways that admin users can access the device</td>
</tr>
<tr>
<td></td>
<td>• Which IP address to use for administering the device from the web</td>
</tr>
<tr>
<td></td>
<td>• Which port the device uses to detect configuration changes made through the web</td>
</tr>
<tr>
<td></td>
<td>• Whether the device automatically emails generated alerts and traffic alarms</td>
</tr>
<tr>
<td></td>
<td>• Whether the device is enabled for reset</td>
</tr>
<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 NetScreen FW/VPN device displays an error message.</td>
</tr>
<tr>
<td>envar</td>
<td>These commands define environment variables. NetScreen FW/VPN 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 NetScreen FW/VPN 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. NetScreen FW/VPN 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>
</tbody>
</table>
Appendix B Unmanaged Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>intervlan-traffic</td>
<td>These commands configure inter-VLAN traffic through a NetScreen FW/VPN 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>ssh</td>
<td>These commands configure the Secure Shell (SSH) server task, an SSH-compatible server application that resides on a NetScreen FW/VPN device. When you enable the SSH server task, SSH client applications can manage the device through a secure connection (the look and feel of an SSH client session is identical to a Telnet session). You can run either SSH version 1 (SSHv1) or SSH version 2 (SSHv2) on a NetScreen FW/VPN device; the commands available depend on the SSH version that you activate.</td>
</tr>
</tbody>
</table>
| set console           | This command defines the CLI console parameters, such as:  
|                       | * Whether the NetScreen FW/VPN device displays messages in the active console window  
|                       | * The number of lines that may appear on a console window page  
|                       | * The maximum time that can pass before automatic logout occurs due to inactivity  
|                       | If console access is currently disabled, you can enable it using the unset console disable command through a Telnet connection. |
| set log audit-loss-mitigation | This command configures logging to mitigate message loss due to memory limitations on a NetScreen FW/VPN device. Used for common criteria only. |
| set mac               | This command configures a static Media Access Control (MAC) address for a NetScreen FW/VPN device interface. |
| timer                 | These commands display timer settings, or configure a NetScreen FW/VPN 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. |
| user                  | These commands create, remove, or display entries in the internal user authentication database. |
Index

A
Abstract Data Model 200
access list, configuring on device 122
active sessions
information available 366
session display filter, configuring 367
session filter, using 366
viewing 365–367
active statistics
device-specific view, described 347
viewing 364
active VPN details 370
activities 52
address objects 208, 277
defined i
administrative reports 436, 440, 443
administrators 50
advanced device options 149
alarms 250
alerts 250
anomaly logs 391
antivirus
See AV
antivirus objects 216
application relocation 251
ARP cache, configuring on device 137
ASN1-DN 292
Atomic Configuration 180
attack object database
checking version on device 194
configuring on device 148
updating on device 194
attack objects
contexts 215
custom 214
defined i
in firewall policies 253
overview 212
protocol anomaly 212
signature 212
updating 213
attack protection
deep inspection alert 254
options 254
severities 254
attack statistics 347, 359–362
attack trends, using reports to identify 446
Attacks By Severity (DI) report 446
Attacks by Severity (DI) report 439
Attacks by Severity (Screen) report 440
Attacks over Time (DI) report 439
Attacks over Time (Screen) report 440, 446
Audit Log Viewer 168, 174
defined i
authentication message, configuring on device 140
authentication server objects
configuring 224
defined ii
authentication servers, configuring default 140
authentication users, configuring on device 153
AV
activating subscription on device 193
configuring external scanner 145
configuring internal scanner 146
configuring on device 145
configuring webmail scanning 146
updating pattern file on device 195

B
backup interface, fail over 198
banners, configuring on device 140
BGP peer, troubleshooting connections to 199
BGP, configuring on device 129
Border Gateway Protocol
See BGP
Index

C
CA certificates, configuring on device 159
categories, logs 405
cell filtering 403
certificate authorities 232
Certificate Revocation List
  See CRL
certificate revocation lists 235
certificates
  CA 159
  configuring on device 156
  CRL configuration 160
  generating request 157
  installing 157
  local 156
  PKI defaults 160
  revocation settings 161
  SCEP 162
  using imported 160
  X509 settings 161
changes that affect device connection 102
chart type, configuring 441
CLI commands, displaying 199
cluster
  See NSRP cluster
configuration logs 396
configuration logs report 439
configuration states 173
Configuration Summary
  running 176, 179
configuring
  devices 101–166, 375–433
  firewall policies 241–262
  objects 205–240
  role-based administration 43–65
  session display filter 367
  session filter for active sessions 366–367
  VPNs 263–336
connection states 172
connections, BGP peer 199
CRL, configuring on device 160
custom attack logs 393

D
Data Model
  defined 201
  importing 203
  schema 201
  updating 201
data point count, configuring 441
date, setting on device 139
Deep Inspection
  activating subscription on device 193
  checking attack object database 194
  configuring on device 147
  see DI
  updating attack object database 194
default authentication servers, configuring on device 140
default values in templates 104
Delta Configuration Summary 177, 179
  running 178, 179
device administration options 139
device capabilities, viewing 118
device capability file 201
device clock, updating 196
device configuration
  overview 102
  unsupported in UI 101
device configuration, updating 179
device connection to Security Manager 102
device groups
  planning for 65
  updating 180
  using 116
device information, configuring 117
device management options 139
Device Manager 38
  using 102
device references, finding 199
Device Server
  overview 33
  processes 34
device statistics 368
device templates 65, 103
  See also templates
device update, errors 185
devices
  upgrading firmware 190
DI reports 436, 439
Diffie-Hellman Group 239
DIP group, creating on device 133
DIP options, configuring on device 138
DIP pool, configuring on device 133
directive
   defined iii
display filter 370
DNS entries, refreshing 196
DNS, configuring on device 137
domain name, configuring on device 151
domain versioning 55

e
e-mail notification, configuring on device 141
entitlement
   See subscription
ethernet statistics
   device-specific view, described 347
   viewing 355–357
export rule, configuring on device 123
exporting a Log Viewer view 413
exporting logs
   to XML 394
external AV scanner, configuring on device 145
external users 278

f
failover
   configuring on interface 135
   forcing on device interface 198
filtering logs 410
   using flags 402
   using ranges 410
Find utility 403
firewall policies 241–262
   assigning to a device 244
   configuring actions 247
   configuring address objects 245
   configuring devices 248
   configuring rule options 248
   configuring rule options, alarms 250
   configuring rule options, alerts 250
   configuring rule options, antivirus 253
   configuring rule options, application relocation 251
   configuring rule options, attack objects 253
   configuring rule options, attack protection 253
   configuring rule options, attack severity 254
   configuring rule options, authentication 252
   configuring rule options, counting 250
   configuring rule options, deep inspection alert 254
   configuring rule options, HA session backup 251
   configuring rule options, logging 250
   configuring rule options, NAT 248
   configuring rule options, protection option 254
   configuring rule options, scan manager 253
   configuring rule options, schedule 251
   configuring rule options, traffic shaping 249
   configuring rule options, URL filtering 251
   configuring rules 245
   configuring services 246
   configuring zones 245
   firewall rules, adding 242
   firewall rules, changing rule order 259
   firewall rules, deleting 259
   firewall rules, disabling 260
   firewall rules, zone exceptions 259
   installing 257
   overview 242
   rule shadowing 255
   rulebases 243
   updating 258
   validating 255
   validation tool 255
   validation, rule duplication 255
   validation, rule shadowing 255
   validation, unsupported options 256
   validation, zone mismatch 255
   VPN links 243
   VPN rules 243
firewall/VPN device
   linking from Log Viewer 417
firmware
   adjusting version on device 191
   upgrading on devices 190
flags in the Log Viewer 402
flow statistics
   device-specific view, described 347
   viewing 357–359
forcing device mode in NSRP cluster 165
FQDN 292
FTP banner, configuring on device 140
FTP server, configuring on device 151
FW/VPN reports 436, 439

G

group expressions 226
  configuring 227
  example 227
group IKE ID 279
group, device 116
GUI Server
  overview 32
  processes 33

H

HA session backup 251
high availability
  device-specific views, described 347
  statistics 368
historical reports 448
host name, configuring on device 151
HTTP banner, configuring on device 140

I

identifying attack trends using reports 446
IKE proposals 238
image file, loading 190
import rule, configuring on device 123
imported certificates, using on device 160
Info options, device configuration 117
information logs 395
information logs report 439
installing license key on device 192
interface
  adding on device 131
  configuring for vsys 155
  configuring on device 132
  device-specific views, described 347
  statistics 355
interface failover
  configuring on device 135
  forcing on device 198
internal AV scanner, configuring on device 146
IP pools 225
IPSec mode 293
ISP settings, configuring on device 136

J

Job Information Window 175, 179, 185
Job Manager
  defined v
  overview 41

K

keep alive frequency 290
key list parameters in templates 104

L

L2TP
  configuring in device-level VPNs 334
  configuring in VPN Manager 285
L2TP user, configuring on device 153
license key
  displaying for device 192
  installing on device 192
  obtaining 192
linking to a device from Log Viewer 417
local certificates, configuring on device 156
local users 278
local users, configuring on device 153
log actions
  csv 394
  email 395
  overview 394
  snmp 394
  syslog 394
  xml 395
log categories 405
log category
  defined vi
log contents
  SCREEN 384
log criteria 395
log destinations
  configuring on device 141
  email server 388
  overview 386
  SNMP 387
Syslog 388
WebTrends server 389
log features 376
log flow 379
Log Investigator 38
defined vi
log modules 378
log severity
   alert 377
   configuring on device 141
critical 377
debugging 377
emergency 377
error 377
information 377
none 377
notification 377
warning 377
log severity levels 377
log sub-categories 405
log types
   alarm 391
   anomaly 383, 391
   config 383
   configuration 396
custom 383
custom attack logs 393
   implicit 383
   info 383
   information 395
SCREEN 384
screen 383
self 383, 385
signature 383, 392
traffic 383, 389
Log Viewer 37
   defined vi
   exporting a view 413
   filtering
      by cell 403
   filtering with flags 402
Find utility 403
   flags 402
   integration with reports 442
   linking to a device 417
   log categories 405
log sub-categories 405
   saving a view 413
   searching by ID 403
   searching using the Find utility 403
   using ranges for filtering 410
   view 413
login message, configuring on device 140
logs
   actions 394
   alarm 391
   checking 173
   configuring on device 141
criteria 394
destinations 386
   enabling in firewall policies 250
filtering 378
   filtering with flags 402
flow of 379
generating 378
modules 378
   searching by ID 403
   searching using the Find utility 403
   severity levels 377
types 382
   using ranges for filtering 410
Logs by User-set Flag report 440, 443
logs, exporting 394

M
   main display area 37
managed devices 34
   management options, configuring on device 139
menu bar 37
messages
   authentication 140
   configuring logging on device 141
   email notification for device 141
   log in 140
   WebAuth login 140
modem settings, configuring on device 136
module, configuring on device 120
modules 37
monitoring
   NSRP statistics 371
   VPN Status 369
multiple devices
  updating 179

N
NACN, configuring on device 134
NAT objects
  DIP objects 230
  in firewall policies 248
  in VPNs 278
  MIP objects 230
  overview 230
  VIP objects 231
NAT Traversal 289
navigation tree 37
NetScreen Address Change Notification
  See NACN
NetScreen Redundancy Protocol
  see NSRP
network options, configuring on device 119
NSM reporting, configuring on device 142
NSRP
  NetScreen Redundancy Protocol, described 371
  statistics monitoring 371
NSRP cluster
  adding members to 164
  configuring 163
  configuring active-active operation 164
  configuring cluster member 164
  creating 163
  forcing device mode 165
  setting cluster ID 163
  synchronizing configurations 165
NSRP Monitor 371
NSRP statistics 347
NTP
  configuring on device 139
  synchronizing device clock 196

O
Object Manager 39
objects
  address objects 208
  antivirus objects 216
  attack objects 212
  attack objects, contexts 215
  attack objects, creating custom 214
  attack objects, protocol anomaly 212
  attack objects, signature 212
  attack objects, updating 213
  authentication servers objects 224
  certificate authorities 232
  certificate revocation lists 235
  group expressions 226
  group expressions, configuring 227
  group expressions, example 227
  IKE proposals 238
  imported 207
  IP pools 225
  NAT objects 230
  NAT objects, DIP objects 230
  NAT objects, MIP objects 230
  NAT objects, VIP objects 231
  overview 206
  protected resources 236
  remote settings 229
  schedule objects 211
  service objects 217
  service objects, custom 218
  service objects, example 219
  types 206
  user objects 221
  user objects, external 222
  user objects, local 221
  using service objects in rules 246
Open Shortest Path First
  See OSPF
  optimizing rulebases using reports 444
  OSPF, configuring on device 126

P
packet flow, configuring on device 151
pattern file, updating on device 195
perfect forward secrecy 239
PKI defaults
  configuring on device 160
  revocation settings 161
  SCEP 162
  X509 certificates 161
policy assignment 244
policy distribution
  device-specific view, described 347
  viewing 348–350
Policy Manager 38
policy merge 65, 244, 260
policy validation tool 255
PPPoE, adding on device 134
predefined entities in templates 104
predefined service timeout, configuring on device 149
primary interface, fail over 198
protected resources 236, 277
protocol anomaly detection, configuring on device 147
protocol distribution
  device-specific view, described 347
  viewing 350–351

R
ranges 410
ranges, filtering with in the Log Viewer 410
Realtime Monitor 40
rebooting devices 196
refreshing DNS entries on devices 196
rekey 293
remote settings 229
replacing a device 198
replay protection 293
report groupings 436
Report Manager 38
report time period, configuring 441
reporting options on device
  email notification 141
  messages and destinations 141
  NSM 142
  SNMP 142
  syslog 143
  Webtrends 143
reports
  administrative 440
  Attacks by Severity (DI) 439
  Attacks by Severity (Screen) 440
  Attacks over Time (DI) 439
  Attacks over Time (Screen) 440
  configuring 441
  DI 439–440
  FW/VPN 439
  historical 448
  Logs by User-set Flag 440
  Screen 440
Top Alarms 439
Top Attackers (Action
  Drop/Close) (DI) 440
Top Attackers (DI) 439
Top Attackers (Screen) 440
Top Attacks (DI) 439
Top Attacks (Screen) 440
Top Configuration Logs 439
Top Information Logs 439
Top Rules 440
Top Self Logs 439
Top Targets (Action
  Drop/Close) (DI) 440
  None) (DI) 440
Top Targets (DI) 440
Top Targets (Screen) 440
Top Traffic Alarms 439
Top Traffic Log 439
using to identify attack trends 446
using to optimize rulebases 444
using to track configuration changes 445
using to track incidents 443
resource statistics
  device-specific view, described 347
  viewing 363–364
restarting devices 196
revocation checking 233
RIP, configuring on device 127
RMA state, setting on device 198
role-based administration
  configuring 50
  creating administrators 50
  creating roles 52
  creating subdomains 55
  domain versioning 55
  example 56
  overview 44
  using effectively 46
  using, enterprise organizations 46
  using, service providers 48
roles
activities 52
assigning 54
custom 52
dependant activities 54
overview 52
root administrator, setting on device 197
route map
configuring on device 122
route preferences, configuring on device 126
Routing Information Protocol
See RIP
routing table, configuring on device 124
rule duplication 255
rule shadowing 255
rulebases, using reports to optimize 444
run-time objects (RTO) 372

S
saving a Log Viewer view 413
scan manager 253
SCEP, configuring on device 162
schedule objects
in firewall policies 251
overview 211
SCREEN log contents 385, 386
SCREEN logs 384
Screen reports 436, 440
ScreenOS firmware
adjusting version on device 191
upgrading on devices 190
searching for logs by ID 403
Security Manager
architecture 31
architecture, Abstract Data Model 200
architecture, Data Model 201
architecture, Data Model schema 201
architecture, device capabilities 200
architecture, Device Server 33
architecture, distributed data collection 34
architecture, GUI Server 32
architecture, managed devices 34
architecture, management system 32
architecture, UI 31
device connection changes 102
modules 37
modules, Audit Log Viewer 41
modules, Device Manager 38
modules, Job Manager 41
modules, Log Investigator 38
modules, Log Viewer 37
modules, Object Manager 39
modules, Policy Manager 38
modules, Realtime Monitor 40
modules, Report Manager 38
modules, Server Manager 40
modules, VPN Manager 39
SSP 35
technical overview 31
UI, main display area 37
UI, menu bar 37
UI, navigation tree 37
UI, overview 36
UI, status bar 37
UI, toolbar 37
Security options, device configuration 145
self logs 385
serial link, configuring on device 135
Server Manager 40
service objects 217
custom 218
example 219
using in rules 246
session filter
configuring 367
configuring to view active sessions 366–367
creating to view active sessions 366
Session Initiation Protocol
See SIP
signature logs 392
Simple Certificate Enrollment Protocol
See SCEP
SIP settings, configuring on device 149
slot, configuring in device 120
SMTP mail server, specifying on device 141
SNMP
configuring on device 142
creating communities 142
source-based routing table, configuring on device 125
SSP 35
startup information, configuring on device 117
status bar 37
sub-categories, logs 405
subdomains 55
subscription, activating 193
synchronizing NSRP configurations 165
syslog reporting
  configuring on device 143
  configuring syslog host 143
system clock, updating 196
system device-specific views 347
system statistics 363

T
Telnet banner, configuring on device 140
templates
  applying 117
  applying multiple templates 108
  applying multiple templates example 108
  benefits 103
  creating 103
  creating and applying example 105
  default values 104
  derived values 106
  key list parameters 104
  modifying applied template 107
  option not supported on device 111
  predefined entities 104
  reverting value to 107
  setting priority level 113
  validating 107
TFTP server, configuring on device 151
time, setting on device 139
timeouts for predefined service, configuring on device 149
toolbar 37
Top Alarms report 439
Top Attackers (Action
  Drop/Close) report 440
Top Attackers (DI) report 439, 447
Top Attackers (Screen) report 440, 446
Top Attacks (DI) report 439
Top Attacks (Screen) report 440, 446
Top Configuration Logs report 439, 445
Top Information Logs report 439
Top Rules report 440, 444
Top Self Logs report 439
Top Targets (Action
  Drop/Close) report 440
  None) report 440
Top Targets (DI) report 440
Top Targets (Screen) report 440, 446
Top Traffic Alarms report 439
Top Traffic Log report 439
tracking configuration changes, using reports 445
tracking incidents, using reports 443
traffic device-specific views 347
traffic log report 439
traffic logs
  conditions 389
  contents 389
  overview 389
traffic shaping 249
  configuring on device 150
troubleshooting
  device, overview 367
  device-specific view, described 347
tunnel interface 280
tunnel zone 280

U
UDP Checksum 290
U-FQDN 292
updating devices
  advantages 168
  event flow 169
  troubleshooting
  device, overview 367
  device-specific view, described 347
upgrading firmware on devices 190
URL filtering 251
  configuring on device 147
user objects
  external 222
  local 221
  overview 221
users, configuring for authentication 153
using flags in the Log Viewer 402
using reports 443–447

V
viewing
  active sessions 365–367
  active statistics 364
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active VPN Details</td>
<td>370</td>
</tr>
<tr>
<td>Active VPN information</td>
<td>354</td>
</tr>
<tr>
<td>attack statistics</td>
<td>359–362</td>
</tr>
<tr>
<td>device traffic distribution</td>
<td>348</td>
</tr>
<tr>
<td>device-specific VPN information</td>
<td>370</td>
</tr>
<tr>
<td>ethernet statistics</td>
<td>355–357</td>
</tr>
<tr>
<td>flow statistics</td>
<td>357–359</td>
</tr>
<tr>
<td>HA statistics</td>
<td>368</td>
</tr>
<tr>
<td>interface statistics</td>
<td>355</td>
</tr>
<tr>
<td>policy distribution</td>
<td>348–350</td>
</tr>
<tr>
<td>resource statistics</td>
<td>363–364</td>
</tr>
<tr>
<td>system statistics</td>
<td>363</td>
</tr>
<tr>
<td>traffic distribution by policy</td>
<td>348</td>
</tr>
<tr>
<td>traffic distribution by protocol</td>
<td>350</td>
</tr>
<tr>
<td>traffic distribution by VPN</td>
<td>352–355</td>
</tr>
<tr>
<td>VPN status summary</td>
<td>369</td>
</tr>
<tr>
<td>zone statistics</td>
<td>363</td>
</tr>
<tr>
<td>VIP options, configuring on device virtual router</td>
<td>138</td>
</tr>
<tr>
<td>adding on device</td>
<td>120</td>
</tr>
<tr>
<td>configuring access list</td>
<td>122</td>
</tr>
<tr>
<td>configuring BGP</td>
<td>129</td>
</tr>
<tr>
<td>configuring export rule</td>
<td>123</td>
</tr>
<tr>
<td>configuring for vsys</td>
<td>154</td>
</tr>
<tr>
<td>configuring import rule</td>
<td>123</td>
</tr>
<tr>
<td>configuring on device</td>
<td>120</td>
</tr>
<tr>
<td>configuring OSPF</td>
<td>126</td>
</tr>
<tr>
<td>configuring RIP</td>
<td>127</td>
</tr>
<tr>
<td>configuring route map</td>
<td>122</td>
</tr>
<tr>
<td>configuring route preferences</td>
<td>126</td>
</tr>
<tr>
<td>configuring routing table entries</td>
<td>124</td>
</tr>
<tr>
<td>configuring source-based routing table</td>
<td>125</td>
</tr>
<tr>
<td>general properties</td>
<td>121</td>
</tr>
<tr>
<td>virtual security devices</td>
<td></td>
</tr>
<tr>
<td>see VSD</td>
<td></td>
</tr>
<tr>
<td>virus pattern file, updating on device</td>
<td>195</td>
</tr>
<tr>
<td>VPN display filter</td>
<td>370</td>
</tr>
<tr>
<td>monitoring status</td>
<td>369</td>
</tr>
<tr>
<td>VPN distribution device-specific view</td>
<td>347</td>
</tr>
<tr>
<td>VPN Manager</td>
<td></td>
</tr>
<tr>
<td>adding policy-based members</td>
<td>284</td>
</tr>
<tr>
<td>adding RAS users</td>
<td>286</td>
</tr>
<tr>
<td>adding routing-based members</td>
<td>286</td>
</tr>
<tr>
<td>adding the VPN</td>
<td>283</td>
</tr>
<tr>
<td>adding the VPN link</td>
<td>297</td>
</tr>
<tr>
<td>autogenerating</td>
<td>294</td>
</tr>
<tr>
<td>configuring ASN1-DN</td>
<td>292</td>
</tr>
<tr>
<td>configuring FQDN</td>
<td>292</td>
</tr>
<tr>
<td>configuring gateway</td>
<td>289</td>
</tr>
<tr>
<td>configuring gateway security</td>
<td>291</td>
</tr>
<tr>
<td>configuring gateway, heartbeats</td>
<td>289</td>
</tr>
<tr>
<td>configuring gateway, mode</td>
<td>289</td>
</tr>
<tr>
<td>configuring gateway, NAT Traversal</td>
<td>289</td>
</tr>
<tr>
<td>configuring IKE IDs</td>
<td>292</td>
</tr>
<tr>
<td>configuring IKE properties</td>
<td>293</td>
</tr>
<tr>
<td>configuring IP address for IKE ID</td>
<td>292</td>
</tr>
<tr>
<td>configuring IPSec mode</td>
<td>293</td>
</tr>
<tr>
<td>configuring L2TP</td>
<td>285</td>
</tr>
<tr>
<td>configuring NAT</td>
<td>284</td>
</tr>
<tr>
<td>configuring NAT with incoming DIP</td>
<td>284</td>
</tr>
<tr>
<td>configuring NAT with MIP, VIP, and Outgoing DIP</td>
<td>285</td>
</tr>
<tr>
<td>configuring NAT with tunnel interface and zone</td>
<td>284</td>
</tr>
<tr>
<td>configuring overrides</td>
<td>295</td>
</tr>
<tr>
<td>configuring overrides, device configuration</td>
<td>296</td>
</tr>
<tr>
<td>configuring overrides, policy rules</td>
<td>295</td>
</tr>
<tr>
<td>configuring Phase 1 proposals</td>
<td>291</td>
</tr>
<tr>
<td>configuring Phase 2 proposals</td>
<td>294</td>
</tr>
<tr>
<td>configuring PKI</td>
<td>291</td>
</tr>
<tr>
<td>configuring preshared key</td>
<td>291</td>
</tr>
<tr>
<td>configuring preshared secrets</td>
<td>292</td>
</tr>
<tr>
<td>configuring termination points</td>
<td>288</td>
</tr>
<tr>
<td>configuring topology</td>
<td>287</td>
</tr>
<tr>
<td>configuring topology, full mesh</td>
<td>288</td>
</tr>
<tr>
<td>configuring topology, hub and spoke</td>
<td>288</td>
</tr>
<tr>
<td>configuring topology, main and branch</td>
<td>288</td>
</tr>
<tr>
<td>configuring topology, site-to-site</td>
<td>288</td>
</tr>
<tr>
<td>configuring U-FQDN</td>
<td>292</td>
</tr>
<tr>
<td>configuring XAuth</td>
<td>290</td>
</tr>
<tr>
<td>creating VPNs</td>
<td>283</td>
</tr>
<tr>
<td>default termination point</td>
<td>283</td>
</tr>
<tr>
<td>editing VPNs</td>
<td>297</td>
</tr>
<tr>
<td>enable</td>
<td>283</td>
</tr>
<tr>
<td>enabling VPN Monitor</td>
<td>293</td>
</tr>
<tr>
<td>enabling VPN Monitor, rekey</td>
<td>293</td>
</tr>
<tr>
<td>examples</td>
<td>298–322</td>
</tr>
<tr>
<td>overview</td>
<td>39, 264</td>
</tr>
<tr>
<td>VPN Monitor</td>
<td>369</td>
</tr>
<tr>
<td>enabling</td>
<td>293</td>
</tr>
</tbody>
</table>