# Part 2

## Chapter 4

### Adding Devices

- **About Device Creation** .................................................. 80
- **Determine Device Status** .............................................. 80
- **Verify Device Configuration** ........................................ 81
- **Managing the Device** ................................................ 81
- **Before You Begin** .......................................................... 82
- **Importing vs. Modeling** ................................................ 82
- **Importing Device Configurations** ............................... 82
- **Modeling Device Configurations** ............................... 83
- **Device Add Process** .................................................. 83
- **Selecting the Domain** ................................................ 84
- **Adding Single or Multiple Devices** ............................. 85
- **Determining ScreenOS Version (ScreenOS only)** .......... 85
- **Determining Port Mode (ScreenOS devices only)** .......... 86
  - **Trust-Untrust Port Mode** .......................................... 86
  - **Home-Work Port Mode** ........................................... 87
  - **Dual-Untrust Port Mode** .......................................... 87
  - **Combined Port Mode** ............................................. 88
  - **Trust-Untrust-DMZ Port Mode** ................................. 89
  - **Trust/Untrust/DMZ (Extended) Mode** ....................... 89
  - **DMZ-Dual-Untrust Port Mode** ................................. 90
- **Port Mode Summary** .................................................. 91
- **Changing the Port Mode** ............................................ 92
- **Importing Devices** .......................................................... 92
  - **Requirements** .......................................................... 92
  - **Adding Devices with Static IP Addresses** .................. 93
    - **ScreenOS 4.0.x Devices** ...................................... 93
    - **ScreenOS 5.x Devices** ......................................... 95
    - **IDP 4.0 Sensors** .................................................. 96
  - **Adding Devices with Dynamic IP Addresses** ............... 97
    - **ScreenOS 4.0.x Devices** ...................................... 97
    - **ScreenOS 5.x Devices** ......................................... 99
    - **IDP 4.0 Sensors** .................................................. 100
- **Verifying Imported Device Configurations** ................. 102
  - **Using Device Monitor** ............................................. 102
  - **Using Device Manager** ........................................... 102
  - **Using Job Manager** ................................................ 103
  - **Using Configuration Summaries (ScreenOS only)** ...... 103
- **Modeling Devices** .......................................................... 104
  - **Requirements** .......................................................... 104
  - **Modeling a Device** ................................................ 105
  - **Creating a Device Configuration** ............................. 106
  - **Activating a Device** .............................................. 106
    - **Devices with Static IP Addresses** ......................... 106
    - **Devices with Dynamic IP Addresses** ..................... 110
  - **Using Rapid Deployment (ScreenOS only)** ................. 113
    - **Overview** ....................................................... 114
    - **Requirements** .................................................. 115
    - **Creating the Configlet** ........................................ 115
    - **Installing the Configlet** ....................................... 118
    - **Preparing the Device** ......................................... 118
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Updating the Attack Object Database</td>
<td>198</td>
</tr>
<tr>
<td>Updating Attacks for IDP-enabled devices</td>
<td>198</td>
</tr>
<tr>
<td>Updating DI Attacks on ScreenOS 5.0 and Lower Devices</td>
<td>200</td>
</tr>
<tr>
<td>Using Updated Attack Objects</td>
<td>201</td>
</tr>
<tr>
<td>Verifying the Attack Database Version</td>
<td>201</td>
</tr>
<tr>
<td>Automatic Verification</td>
<td>201</td>
</tr>
<tr>
<td>Manual Verification</td>
<td>202</td>
</tr>
<tr>
<td>Managing Different Attack Database Versions</td>
<td>202</td>
</tr>
<tr>
<td>Updating the IDP Detector Engine</td>
<td>203</td>
</tr>
<tr>
<td>Scheduling Security Updates</td>
<td>204</td>
</tr>
<tr>
<td>Scheduling the Update</td>
<td>206</td>
</tr>
<tr>
<td>Viewing Scheduled Security Updates in the Job Manager</td>
<td>208</td>
</tr>
<tr>
<td>Viewing Scheduled Security Updates in the Audit Log Viewer</td>
<td>208</td>
</tr>
<tr>
<td>Updating AV Pattern Files</td>
<td>208</td>
</tr>
<tr>
<td>Updating the Web Category List</td>
<td>209</td>
</tr>
<tr>
<td>Miscellaneous Device Operations</td>
<td>209</td>
</tr>
<tr>
<td>Restarting Devices</td>
<td>210</td>
</tr>
<tr>
<td>Refreshing DNS Entries</td>
<td>210</td>
</tr>
<tr>
<td>Updating the Device Clock with an NTP Server</td>
<td>211</td>
</tr>
<tr>
<td>Setting the Root Administrator on a Device</td>
<td>211</td>
</tr>
<tr>
<td>Failing Over/Reverting Back Interfaces</td>
<td>212</td>
</tr>
<tr>
<td>Setting RMA State on a Device</td>
<td>213</td>
</tr>
<tr>
<td>Troubleshooting a BGP Peer Session on a Device</td>
<td>213</td>
</tr>
<tr>
<td>Displaying CLI Commands on a Device</td>
<td>214</td>
</tr>
<tr>
<td>Reactivating Wireless Connections</td>
<td>214</td>
</tr>
<tr>
<td>Finding Usages</td>
<td>214</td>
</tr>
<tr>
<td>Managing Device Capabilities</td>
<td>214</td>
</tr>
<tr>
<td>Abstract Data Model</td>
<td>215</td>
</tr>
<tr>
<td>Data Model</td>
<td>215</td>
</tr>
<tr>
<td>Data Model Schema</td>
<td>216</td>
</tr>
<tr>
<td>Data Model Updating</td>
<td>216</td>
</tr>
<tr>
<td>Data Model Importing</td>
<td>218</td>
</tr>
<tr>
<td>Archiving and Restoring</td>
<td>219</td>
</tr>
<tr>
<td>Archiving Logs and Configuration Data</td>
<td>219</td>
</tr>
<tr>
<td>Restoring Logs and Configuration Data</td>
<td>220</td>
</tr>
</tbody>
</table>

Part 3  Managing

Chapter 8 Configuring Objects  223

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About Objects</td>
<td>225</td>
</tr>
<tr>
<td>Importing Objects from Global-PRO</td>
<td>226</td>
</tr>
<tr>
<td>Using Objects Across Domains</td>
<td>227</td>
</tr>
<tr>
<td>Configuring Address Objects</td>
<td>227</td>
</tr>
<tr>
<td>Viewing Address Objects</td>
<td>227</td>
</tr>
<tr>
<td>Creating Address Objects</td>
<td>228</td>
</tr>
<tr>
<td>Adding a Host Address Object</td>
<td>228</td>
</tr>
<tr>
<td>Adding a Network Address Object</td>
<td>229</td>
</tr>
<tr>
<td>Editing and Deleting Address Objects</td>
<td>229</td>
</tr>
<tr>
<td>Replacing Address Objects</td>
<td>229</td>
</tr>
<tr>
<td>Adding an Address Object Group</td>
<td>229</td>
</tr>
<tr>
<td>Adding a Multicast Group Address Object</td>
<td>230</td>
</tr>
</tbody>
</table>
Adding Static DNS Host Addresses ................................................................. 231
Blocked Hosts .............................................................................................. 232
Configuring Schedule Objects ......................................................................... 232
Creating Schedule Objects ........................................................................... 233
Working With DI Attack Objects .................................................................... 233
Viewing Predefined DI Attack Objects ........................................................... 234
Viewing Attack Version Information for Attack Objects ................................ 234
Viewing Predefined DI Attack Object Groups .............................................. 234
Updating Predefined DI Attack Objects and Groups ...................................... 235
Creating DI Profiles ..................................................................................... 235
Working with IDP Attack Objects ................................................................... 237
Viewing Predefined IDP Attacks ..................................................................... 237
Viewing Predefined IDP Attack Groups ........................................................ 239
Viewing Attack Version Information for Attack Objects and Groups .......... 239
Updating Predefined IDP Attack Objects and Groups ..................................... 240
Configuring Custom DI/IDP Attacks ............................................................... 240
Using the Attack Object Wizard .................................................................... 240
Copying/Editing Predefined Attack Objects to Create Custom Attack Objects 241
Configuring Attack Name and Description .................................................... 241
Configuring Extended Information ................................................................. 242
Configuring External References ................................................................... 243
Configuring Target Platforms ......................................................................... 243
Creating a Signature Attack Object ................................................................. 245
Configuring General Attack Properties ........................................................ 245
Configuring Attack Detection Properties ....................................................... 248
Configuring Header Match Properties .......................................................... 251
Configuring a Protocol Anomaly Attack Object ............................................ 255
Configuring a Compound Attack Object ........................................................ 255
Configuring General Attack Properties ........................................................ 256
Configuring Compound Attack Members ...................................................... 256
Configuring Direction Filter ............................................................................ 258
Creating Custom DI Attack Groups ............................................................... 258
Creating Custom IDP Attack Groups ............................................................. 259
Creating Static Attack Groups ....................................................................... 259
Creating Dynamic Attack Groups (IDP Only) ............................................... 260
Updating Dynamic Groups ............................................................................ 262
Editing a Custom Attack Group ..................................................................... 263
Deleting a Custom Attack Group ................................................................. 263
Configuring Custom Policy Fields ................................................................. 263
Defining Metadata ........................................................................................ 264
Instantiating New Objects ............................................................................. 264
Adding Custom Detail Object to Rules .......................................................... 264
Open Log Viewer ........................................................................................... 265
Configuring AntiVirus Objects ...................................................................... 265
Configuring External AV Profiles ................................................................. 265
Configuring Internal AV Profiles .................................................................... 266
View the Predefined Profile .......................................................................... 266
Create Custom AV Profiles ........................................................................... 266
Configuring Extension Lists .......................................................................... 267
Configuring Mime Lists ................................................................................ 268
Configuring ICAP AV Servers and Profiles ................................................... 268
Configuring ICAP AV Servers and Server Groups ......................................... 268
Configuring ICAP AV Profiles ....................................................................... 269
Configuring Web Filtering Objects ............................................................... 270
Web Categories ..................................................................................... 271
Custom Lists ................................................................................... 271
Predefined Categories ..................................................................... 272
Web Profiles .................................................................................. 273
Custom Profiles ............................................................................... 273
Predefined Profiles .......................................................................... 274
Configuring GTP Objects .............................................................................. 275
Configuring Info .................................................................................... 275
Limiting GTP Message Length .......................................................... 275
Limiting GTP Message Rate .............................................................. 275
Limiting GTP Tunnels ...................................................................... 276
Removing Inactive GTP Tunnels ..................................................... 276
Validating Sequence Numbers ......................................................... 276
Filtering GTP-in-GTP Packets ........................................................... 277
Removing GTP R6 Informational Elements ..................................... 277
Inspecting Tunnel Endpoint IDs ...................................................... 277
Configuring Traffic Logging and Counting.............................................. 277
Traffic Counting .............................................................................. 277
Traffic Logging ................................................................................ 278
Configuring IMSI Prefix and APN Filtering ............................................. 278
Creating an APN Filter ..................................................................... 278
Creating an IMSI Prefix Filter .......................................................... 279
Configuring GTP Message Filtering ........................................................ 280
Configuring Subscriber Tracing (Lawful Interception) ....................... 280
Configuring Service Objects ......................................................................... 281
Viewing Predefined Services ............................................................... 282
Creating Custom Services ...................................................................... 283
Service Object Groups ........................................................................ 284
Editing and Deleting Service Objects ..................................................... 288
Replacing Service Objects ...................................................................... 288
Configuring Authentication Servers.............................................................. 289
Configuring General Authentication Server Settings............................... 289
Configuring Authentication Server Redundancy .................................... 290
Configuring Authentication for User Types ............................................ 290
Domain Name Checking ................................................................. 290
Domain Name Stripping .................................................................. 291
Configuring Authentication Server Types ............................................. 291
Configuring a RADIUS Authentication Server .................................. 292
Configuring a SecurID Authentication Server .................................. 296
Configuring an LDAP Authentication Server .................................... 297
Configuring User Objects ............................................................................. 298
Configuring Local Users ......................................................................... 298
Configuring Local User Groups ............................................................... 298
Configuring External Users .................................................................... 299
Configuring External User Groups .......................................................... 299
Configuring VLAN Objects ............................................................................ 302
Configuring IP Pools..................................................................................... 303
Using Multiple IP Ranges ....................................................................... 303
Configuring Group Expressions .......................................................... 304
Configuring Group Expressions .......................................................... 305
Configuring Remote Settings .............................................................. 307
Configuring NAT Objects .......................................................................... 308
Configuring DIP Objects .......................................................................... 308
Comments For Firewall Rules................................................................. 346
Configuring Multicast Rules................................................................. 347
Configuring Source and Destination Zones........................................ 347
Configuring Source and Destination Groups..................................... 347
Configuring Rule Options................................................................. 347
Configuring Antivirus Rules............................................................... 349
Configuring Antispam Rules............................................................... 350
Configuring IDP Rules........................................................................ 350
Defining Match For IDP Rules............................................................ 351
  Configuring Source & Destination Zones for IDP Rules (Does not apply to Standalone IDP Sensor rulebases).................................................................................................................. 351
  Configuring Source & Destination Address Objects for IDP Rules.... 351
  Configuring Services for IDP Rules................................................. 352
  Configuring Terminal IDP Rules..................................................... 355
Defining Actions For IDP Rules........................................................... 356
Configuring Attack Objects in IDP Rules.......................................... 357
  Adding IDP Attack Object Groups by Category............................ 358
  Adding IDP Attack Objects by Operating System......................... 358
  Adding IDP Attack Objects by Severity......................................... 358
  Adding Custom Dynamic Attack Groups..................................... 359
Configuring IP Actions in IDP Rules................................................... 359
  Choosing an IP Action.................................................................... 359
  Choosing a Block Option.............................................................. 360
  Setting Logging Options.............................................................. 360
  Setting Timeout Options............................................................... 360
Configuring Notification in IDP Rules.............................................. 360
  Setting VLAN Tags for IDP Rules................................................ 361
  Setting Severity for IDP Rules..................................................... 362
  Setting Target Security Devices for IDP Rules............................ 362
  Entering Comments for IDP Rules............................................... 363
Configuring Exempt Rules.................................................................. 364
  Adding the Exempt Rulebase......................................................... 364
  Defining Match.............................................................................. 364
    Configuring Source & Destination Zones................................... 365
    Configuring Source & Destination Address Objects............... 365
    Setting Attack Objects.............................................................. 365
    Specifying VLANs ...................................................................... 366
    Setting Target Devices.............................................................. 366
    Entering Comments................................................................. 366
    Creating an Exempt Rule from the Log Viewer......................... 366
Configuring Backdoor Rules............................................................... 367
  Adding the Backdoor Rulebase...................................................... 368
  Defining Match.............................................................................. 368
    Configuring Source & Destination Zones................................. 369
    Configuring Source & Destination Address Objects............... 369
    Configuring Services............................................................... 369
    Setting Operation...................................................................... 369
    Setting Actions......................................................................... 370
    Setting Notification.................................................................... 370
    Setting Logging......................................................................... 370
    Setting an Alert.......................................................................... 370
    Logging Packets......................................................................... 371
    Setting Severity......................................................................... 371
    Specifying VLANs....................................................................... 371
Contents

NetScreen-Security Manager 2007.2 Administrator's Guide

Setting Target Devices ................................................................. 371
Entering Comments................................................................. 371
Configuring SYN Protector Rules ........................................... 372
  The TCP Handshake............................................................... 372
  SYN-Floods........................................................................... 372
Adding the SYN Protector Rulebase......................................... 373
Defining Match........................................................................... 373
  Configuring Source & Destination Address Objects ............ 373
  Configuring Services ......................................................... 374
Setting Mode ............................................................................. 374
Setting Notification................................................................. 374
  Setting Logging................................................................. 375
  Setting an Alert ............................................................... 375
  Logging Packets ............................................................... 375
Setting Severity......................................................................... 376
Specifying VLANs ................................................................. 376
Setting Target Devices ............................................................. 376
Entering Comments................................................................. 376
Configuring Traffic Anomalies Rules........................................ 376
  Detecting TCP and UDP Port Scans................................. 377
  Detecting Other Scans........................................................ 377
  Session Limiting............................................................... 378
Adding the Traffic Anomolies Rulebase.................................... 379
Defining Match......................................................................... 379
  Configuring Source & Destination Address Objects ............ 379
  Configuring Services ......................................................... 379
Setting Detect Options............................................................ 379
Setting Response Options........................................................ 380
Setting Notification................................................................. 380
  Setting Logging................................................................. 380
  Setting an Alert ............................................................... 381
  Logging Packets ............................................................... 381
Setting Severity......................................................................... 381
Specifying VLANs ................................................................. 381
Setting Target Devices ............................................................. 381
Entering Comments................................................................. 381
Configuring Network Honeypot Rules...................................... 382
  Impersonating a Port ........................................................ 382
Adding the Network Honeypot Rulebase.................................. 382
Defining Match......................................................................... 383
  Configuring Source............................................................ 383
  Configuring Destination Address Objects and Services ..... 383
Setting Operation................................................................. 383
Setting Response Options........................................................ 383
Setting Notification................................................................. 383
  Setting Logging................................................................. 383
  Setting an Alert ............................................................... 384
  Logging Packets ............................................................... 384
Setting Severity......................................................................... 384
Specifying VLANs ................................................................. 384
Setting Target Devices ............................................................. 384
Entering Comments................................................................. 385
Installing Security Policies....................................................... 385
Assigning a Security Policy to a Device................................. 385
Using IPSec ........................................................................................................ 421
Using L2TP ........................................................................................................ 423
Choosing a VPN Tunnel Type ........................................................................ 423
About Policy-Based VPNs ............................................................................... 424
About Route-Based VPNs ............................................................................... 424
VPN Checklist .................................................................................................. 424
Define Members and Topology ...................................................................... 424
Define VPN Type: Policy-Based, Route-Based, or Mixed-Mode .................. 425
Define Security Protocol (Encryption and Authentication) ......................... 425
Define Method: VPN Manager or Device-Level? .......................................... 425
Preparing VPN Components ........................................................................... 427
Preparing Basic VPN Components ................................................................. 427
Preparing Required Policy-Based VPN Components ................................... 428
Configuring Address Objects ......................................................................... 428
Configuring Protected Resources .................................................................. 428
Configuring Shared NAT Objects .................................................................. 429
Configuring Remote Access Service (RAS) Users ......................................... 429
Configuring Required Routing-Based VPN Components ............................. 431
Configuring Tunnel Interfaces and Tunnel Zones .......................................... 431
Configuring Static and Dynamic Routes ......................................................... 432
Configuring Optional VPN Components ........................................................ 432
Creating Authentication Servers .................................................................... 433
Creating Certificate Objects ........................................................................... 433
Creating PKI Defaults .................................................................................... 434
Creating VPNs with VPN Manager ................................................................. 434
Adding the VPN ............................................................................................. 435
Configuring Members ..................................................................................... 435
Adding Policy-Based Members ....................................................................... 436
Adding RAS Users .......................................................................................... 436
Adding Routing-Based Members ..................................................................... 438
Configuring Topology ..................................................................................... 440
Configuring Common VPN Topologies ......................................................... 441
Defining Termination Points ........................................................................... 442
Configuring Gateways ..................................................................................... 442
Configuring Gateway Properties .................................................................... 442
Configuring Gateway Security ....................................................................... 444
Configuring IKE IDs ........................................................................................ 445
Configuring IKE ............................................................................................. 446
IKE Properties ................................................................................................. 446
Configuring Security Level ............................................................................. 447
Autogenerating VPN Rules ............................................................................. 448
Configuring Overrides .................................................................................... 448
Editing Policy Rules ........................................................................................ 448
Editing Device Configuration .......................................................................... 449
Viewing the Device Tunnel Summary ............................................................. 450
Adding the VPN Link ....................................................................................... 450
Editing VPNs ................................................................................................... 451
Editing VPN Protected Resources ................................................................... 451
Editing Users .................................................................................................. 451
Editing the VPN Configuration ....................................................................... 451
Editing VPN Overrides .................................................................................... 451
VPN Manager Examples .................................................................................. 452
Creating Device-Level VPNs .......................................................................... 474
Supported Configurations ............................................................................. 475
### Creating AutoKey IKE VPNs
- Configuring Gateways: 475
- Configuring Routes (Route-based only): 479
- Configuring the VPN: 480
- Adding a VPN Rule: 482

### Creating Manual Key VPNs
- Adding XAuth Users: 483
- Configuring Routes (Route-based only): 483
- Configuring the VPN: 483
- Adding a VPN Rule: 485

### Creating L2TP VPNs
- Adding L2TP Users: 486
- Configuring L2TP: 486
- Adding a VPN Rule: 487

### Creating L2TP Over Autokey IKE VPNs
- Adding VPN Rules: 488
- Configuring the VPN: 488
- Configuring the Security Policy: 488
- Assign and Install the Security Policy: 489

### Device-Level VPN Examples
- Chapter 11 Central Manager
  - Central Manager Overview: 504
    - Regional Server and Central Manager Self-Sufficiency: 505
      - Self-Sufficient Central Manager: 505
      - Self-Sufficient Regional Server: 505
    - Super Admin User: 505
    - Regional Server Management: 505
      - Using Central Manager: 506
        - Adding a Regional Server Object: 506
        - Deleting a Regional Server Object: 508
        - Logging into a Regional Server: 508
  - Installing Global Policy to a Regional Server: 510
    - Pre/Post Rules update during Global Policy Install: 511
    - Shared Objects Update During Global Policy Install: 511
    - Name Space Conflict Resolution for Shared Objects: 511
    - Name Space Conflict Resolution for Polymorphic Objects: 512

### Part 4 Monitoring

#### Chapter 12 Realtime Monitoring
- About the Realtime Monitor: 516
- Realtime Monitor Views: 516
- Monitoring Security Devices: 517
  - Viewing Device Status: 517
  - Device Polling Intervals: 519
- Viewing Additional Device Detail and Statistics: 520
  - Viewing Device Details: 520
  - Viewing Device Statistics: 522
- Monitoring IDP Sensors: 541
Contents

NetScreen-Security Manager 2007.2 Administrator's Guide

Viewing IDP Device Status ................................................................. 541
Viewing IDP Device Detail and Statistics ......................................... 542
Viewing IDP Device Details ............................................................... 542
Viewing IDP Process Status ............................................................. 543
Viewing IDP Device Statistics .......................................................... 544

Monitoring VPNs ................................................................................ 545
Viewing the VPN Status Summary .................................................. 545
Configuring a VPN Display Filter ................................................... 546
Viewing Active VPN Details ............................................................ 546
Viewing Device-Specific VPN Information ....................................... 546

Monitoring NSRP Statistics .............................................................. 547
Viewing NSRP Summary Information .............................................. 547
Viewing VSD/RTO Information ....................................................... 547
Viewing VSD Counter Details .......................................................... 548
Viewing RTO Counter Details .......................................................... 549

Monitoring IDP Clusters .................................................................. 549
Viewing IDP Cluster Summary Information ..................................... 550
Monitoring IDP Cluster Members .................................................... 551

Using The Realtime Monitor............................................................. 551
Monitoring the Management System .............................................. 552
Configuring Servers ........................................................................ 552
Configuring Device Servers ............................................................ 553
Configuring the GUI Server ............................................................. 553
Using Server Monitor ...................................................................... 554
Viewing Server Status .................................................................... 554
Viewing Additional Server Status Details ....................................... 555
Viewing Process Status ................................................................... 557

Using Management System Utilities ................................................. 558

Chapter 13 Analyzing Your Network ................................................. 561

About the Dashboard ....................................................................... 562
About the Profiler ............................................................................ 562
Setting Up the Profiler .................................................................... 563
   Enabling OS Fingerprinting ......................................................... 564
   Configuring Network Objects ....................................................... 565
   Configuring Context Profiles ....................................................... 565
   Configuring Alerts ...................................................................... 566
Updating Profiler Settings ................................................................ 566
Starting the Profiler ....................................................................... 566
Stopping the Profiler ...................................................................... 567
Customizing Profiler Preferences ................................................... 567

About Profiler Views ....................................................................... 567
About the Application Profiler ....................................................... 568
About the Network Profiler ............................................................ 569
About the Violation Viewer ............................................................. 570
   Configuring Permitted Objects ..................................................... 571
Using Profiler Views ....................................................................... 572
   Filtering and Sorting ................................................................... 573
   Refreshing Profiler Data ............................................................. 574
   Viewing DB Information .............................................................. 574
   Viewing Detailed Network Information ....................................... 574

Recommended Profiler Options ....................................................... 576
Configuring a Network Baseline ..................................................... 576
Identifying a Baseline ..................................................................... 576
### Setting a Baseline
- Keeping Your Network Current .......................................................... 577
- Proactively Updating Your Network ...................................................... 577
- Reacting to Vulnerability Announcements ........................................... 578
- Stopping Worms and Trojans ............................................................... 578
  - Example: SQL Worm ........................................................................ 578
  - Example: Blaster Worm .................................................................. 579

### Accessing Data in the Profiler DB
- About Security Explorer ........................................................................ 580
  - Security Explorer Main Graph ......................................................... 581
  - Graph Types .................................................................................. 582
  - Connections Detail Pane ................................................................. 583
  - Reference Point Pane ...................................................................... 583
  - Log Viewer .................................................................................... 583
  - Reports Viewer ............................................................................... 583
- Using Security Explorer .......................................................................... 584
  - Permissions ................................................................................... 584
  - Analyzing Relationships .................................................................. 585
    - Viewing Data .............................................................................. 585
    - Transitioning to Other Relational Graphs ..................................... 585
    - Setting a Time Duration ............................................................... 586
    - Viewing Predefined Reports ........................................................ 586
    - Refreshing Data ........................................................................... 586
    - Adding and Removing Panels ...................................................... 586
  - Exporting to HTML ........................................................................... 586

### Chapter 14: Logging
- About Logging .................................................................................... 588
  - About Log Entries .......................................................................... 588
  - About Log Events ........................................................................... 588
  - About Log Severity ......................................................................... 589
- Viewing Logs ........................................................................................ 590
- Configuring Logging ............................................................................ 590
  - Configuring the Device for Logging ............................................... 591
    - Configuring Severity Settings ..................................................... 591
    - Configuring Email Server Settings .............................................. 593
    - Configuring Events Reporting Settings ...................................... 593
    - Configuring SNMP Reporting Settings ....................................... 599
    - Directing Logs to a Syslog Server .............................................. 600
    - Directing Data to a WebTrends Server ....................................... 601
- Using the Log Viewer ........................................................................... 601
  - Using Log Views ............................................................................ 602
    - About Predefined Log Views ....................................................... 602
    - Creating Custom Views and Folders ............................................ 603
    - Creating Per Session Views ......................................................... 604
    - Log Viewer Columns ................................................................. 604
    - Log Viewer Detail Panes ............................................................. 607
    - Log Viewer Status Bar ............................................................... 607
    - Navigating the Log Viewer ......................................................... 607
  - Searching Log Entries ....................................................................... 608
    - Log Timeline ............................................................................... 609
    - Using Flags ................................................................................ 611
    - Using the Find Utility .................................................................. 611
    - Using Log ID Number ................................................................ 612
### Using the Log2Action Utility to Export Logs
- Using Filters .............................................................. 643
- Exporting to XML .................................................... 645
- Using XML Required/Optional Format—Specify Filters .... 645
- Viewing XML Format Output .................................... 645
- Exporting to CSV .................................................... 646
- Using CSV Required/Optional Format—Specify Filters .... 646
- Viewing CSV Format Output .................................... 646
- Exporting to SNMP .................................................. 647
- Using SNMP Required/Optional Format—Specify Filters .... 647
- Viewing SNMP Format Output ................................. 647
- Exporting to Email .................................................. 648
- Using Email Required/Optional Format—Specify Filters .... 648
- Exporting to syslog ............................................... 648
- Using Syslog Required/Optional Format—Specify Filters .... 649
- Viewing Syslog Format Output ................................ 649
- Exporting to a Script ............................................... 649
- Using Script Required/Optional Format—Specify Filters .... 649

### Chapter 15 Reporting

#### About Reporting ................................................................. 652
- Report Type Groupings .................................................. 652
- Graphical Data Representation ........................................ 653
- Integration with Logs ..................................................... 653
- Central Access to Management Information..................... 653

#### Report Types ................................................................. 653
- Predefined Reports ...................................................... 653
  - Firewall/VPN Reports .................................................. 654
  - DI/IDP Reports ......................................................... 654
  - Screen Reports .......................................................... 655
  - Administrative Reports ............................................. 655
  - UAC Reports .............................................................. 656
- My Reports .................................................................... 656
- Shared Reports ............................................................ 656

#### Working with Reports ....................................................... 656
- Generating a Predefined Report ...................................... 657
- Creating a Custom Report ............................................. 657
- Deleting Reports ......................................................... 657
- Organizing Reports in Folders ........................................ 657
- Generating Reports Automatically .................................. 658
  - Running Reports Using the guiSvrCLI.sh Utility .............. 659
  - Creating and Editing Action Scripts ................................ 659
- Using Cron with Scheduled Reports ............................. 660
- Exporting Reports to HTML .......................................... 662

#### Setting Report Options .................................................... 663
- Naming a Report ........................................................ 663
- Setting the Report Type ............................................... 663
- Configuring Report Source Data .................................... 663
- Configuring a Report Time Period ................................. 664
- Configuring the Data Point Count ............................... 664
- Configuring the Chart Type .......................................... 664
- Sharing Your Custom Report ......................................... 664
- Modifying Report Filters ............................................ 664
- Configuring Report Processing Warnings ....................... 665
### Contents

- Saving Your Report Settings ................................................................. 665
- Log Viewer Integration ........................................................................ 665
- Viewing Logs From Report Manager .................................................. 665
- Generating Quick Reports ................................................................. 666
- Using Reports ...................................................................................... 667
- Using Statistical Reports ................................................................. 672
- Using the Watch List ........................................................................... 672

#### Part 5 Appendixes

<table>
<thead>
<tr>
<th>Appendix</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appendix A</td>
<td>Glossary</td>
<td>675</td>
</tr>
<tr>
<td>Appendix B</td>
<td>Unmanaged ScreenOS Commands</td>
<td>695</td>
</tr>
<tr>
<td>Appendix C</td>
<td>SurfControl Web categories</td>
<td>697</td>
</tr>
<tr>
<td>Appendix D</td>
<td>Common Criteria EAL2 Compliance</td>
<td>703</td>
</tr>
<tr>
<td></td>
<td>Guidance for Intended Usage</td>
<td>703</td>
</tr>
<tr>
<td></td>
<td>Guidance for Personnel</td>
<td>703</td>
</tr>
<tr>
<td></td>
<td>Guidance for Physical Protection</td>
<td>703</td>
</tr>
<tr>
<td>Appendix E</td>
<td>Log Entries</td>
<td>705</td>
</tr>
<tr>
<td></td>
<td>Screen Alarm Log Entries</td>
<td>706</td>
</tr>
<tr>
<td></td>
<td>Alarm Log Entries</td>
<td>707</td>
</tr>
<tr>
<td></td>
<td>Deep Inspection Alarm Log Entries</td>
<td>708</td>
</tr>
<tr>
<td></td>
<td>Configuration Log Entries</td>
<td>773</td>
</tr>
<tr>
<td></td>
<td>Information Log Entries</td>
<td>775</td>
</tr>
<tr>
<td></td>
<td>Self Log Entries</td>
<td>776</td>
</tr>
<tr>
<td></td>
<td>Traffic Log Entries</td>
<td>776</td>
</tr>
<tr>
<td></td>
<td>GTP Log Entries</td>
<td>776</td>
</tr>
</tbody>
</table>

#### Part 6 Index

Index ........................................................................................................ 781
List of Figures

Figure 1: UI Navigation Example .............................................................. xxxii
Figure 2: Graphic Conventions................................................................. xxxiii
Figure 1: NetScreen-Security Manager Network Architecture ....................... 12
Figure 2: NetScreen-Security Manager System Architecture .......................... 13
Figure 3: Overview of the User Interface ..................................................... 18
Figure 4: UI Search Modes ........................................................................... 25
Figure 5: “Contains String” Search Mode Example ...................................... 26
Figure 6: “Starts With” Search Mode Example ............................................. 27
Figure 7: “Regular Expression” Search Mode Details ................................... 27
Figure 8: “Regular Expression” Search Mode Example ................................ 28
Figure 9: “IP Address” Search Mode Example ............................................ 29
Figure 10: Select the GUI Server in Central Manager................................. 48
Figure 11: Setting Up an Information Banner ............................................. 49
Figure 12: Information Banner Login Into Central Manager ....................... 49
Figure 13: Access Denied to GUI Server.................................................... 50
Figure 14: Creating Custom Domain............................................................ 61
Figure 15: User in domain “global” with a pre-defined role ......................... 62
Figure 16: User in domain “global” with custom role “r1” ............................ 62
Figure 17: User in subdomain “d1” with a pre-defined role ......................... 63
Figure 18: User in sub-domain “d1” with a custom role “r1” ....................... 63
Figure 19: Assigning multiple roles to a user in global domain .................. 63
Figure 20: Assigning multiple roles to a user in sub-domain ...................... 64
Figure 21: Assigning roles defined in domain “global” .............................. 64
Figure 22: Assigning roles defined in domain “global” to sub-domain only ... 64
Figure 23: Manage Administrators and Domains: Administrators Tab .......... 74
Figure 24: Connecting Devices from Different Domains in VPNs................. 84
Figure 25: Trust-Untrust Port Mode Bindings ............................................. 86
Figure 26: Home-Work Port Mode Bindings .............................................. 87
Figure 27: Dual-Untrust Port Mode Bindings ............................................. 88
Figure 28: Combined Port Mode Bindings ............................................... 88
Figure 29: Trust-Untrust-DMZ Port Mode Bindings .................................. 89
Figure 30: Extended Port-Mode Interface to Zone Bindings ....................... 90
Figure 31: DMZ Dual Untrust Port Mode .................................................. 90
Figure 32: Connecting Vsys Devices Across Domains ................................ 123
Figure 33: Configuring Cluster Members for Paris Vsys Cluster .................. 129
Figure 34: View Template Override Message .......................................... 150
Figure 35: Revert to a Template or Default Value ..................................... 151
Figure 36: Template Operations Dialog ................................................... 154
Figure 37: Select Template Dialog ......................................................... 155
Figure 38: Template Operations Job Information Dialog ......................... 157
Figure 39: View Denial of Service Defense Values from DoS Template ....... 161
Figure 40: Configure DoS Defense Settings for the DoS2 Template .......... 162
Figure 41: View Template Priority (DoS Highest) .................................... 162
Figure 42: Set Template Priority (DoS2 Highest) ...................................... 163
Figure 43: View Values from DoS and DoS2 Templates ........................................ 163
Figure 44: View DoS2 Value for Source IP Based Session Limit ........................ 164
Figure 45: View DoS Value for SYN-ACK-ACK Proxy Protection Setting ........... 164
Figure 46: View Default SYN-ACK-ACK Proxy Protection Setting....................... 164
Figure 47: Delta Configuration Summary Example............................................ 184
Figure 48: Delta Configuration Summary Example............................................ 185
Figure 49: Job Manager Module......................................................................... 189
Figure 50: Job Information Dialog Box............................................................. 190
Figure 51: Failed Update Job Dialog Box.......................................................... 192
Figure 52: Attack Update Summary................................................................. 204
Figure 53: Import/Update Architecture............................................................ 215
Figure 54: Data Model Update........................................................................... 217
Figure 55: Data Model Importing...................................................................... 218
Figure 56: Attack Viewer................................................................................... 238
Figure 57: New Dynamic Group........................................................................ 261
Figure 58: New Dynamic Group Members....................................................... 262
Figure 59: Create New Custom URL List......................................................... 272
Figure 60: Changing Default Action for WebWeb Profile Category..................... 274
Figure 61: RADIUS Authentication Server Overview........................................ 292
Figure 62: Configure RADIUS Auth Server..................................................... 295
Figure 63: Configure Firewall Rule To Authenticate Accountant Access............. 302
Figure 64: VLAN Object Dialog......................................................................... 302
Figure 65: Configure External User Groups For Sales and Marketing................... 306
Figure 66: Configure Group Expression for Sales and Marketing....................... 307
Figure 67: Configure Rule Options to Authenticate Sales and Marketing.............. 307
Figure 68: Protected Resource Overview.......................................................... 314
Figure 69: Set Individual Sources and Destinations in a Firewall Rule................... 332
Figure 70: Set Group Sources and Destinations in a Firewall Rule...................... 333
Figure 71: Negate Source in a Firewall Rule..................................................... 333
Figure 72: Set Standard Services in a Firewall Rule............................................ 334
Figure 73: Set Custom Services in a Firewall Rule............................................. 334
Figure 74: Configure Web Filtering in a Firewall Rule........................................ 343
Figure 75: Configure Source/Destination for Multicast Rule.............................. 349
Figure 76: Set Source and Destination............................................................... 352
Figure 77: Set Multiple Source and Destination Networks .................................... 352
Figure 78: Set Default Services......................................................................... 353
Figure 79: Set Custom Services........................................................................ 353
Figure 80: Add Non-Standard Services Object.................................................. 354
Figure 81: Set Non-Standard Service............................................................... 355
Figure 82: Set Terminal Rules.......................................................................... 356
Figure 83: VLAN Tags in a Rule........................................................................ 362
Figure 84: Firewall Rule for Dedicated IDP....................................................... 363
Figure 85: IDP Rules for Dedicated IDP............................................................ 363
Figure 86: Exempting Source and Destination.................................................. 365
Figure 87: Exempting Attack Object............................................................... 366
Figure 88: Exempting a Log Record Rule........................................................ 367
Figure 89: SYN Protector Rulebase................................................................. 373
Figure 90: Setting the Session Limit Options.................................................... 378
Figure 91: Traffic Anomalies Rulebase.............................................................. 379
Figure 92: Configuring IP Action...................................................................... 380
Figure 93: Network Honeypot Rulebase............................................................ 383
Figure 94: Rule Duplication Example.............................................................. 387
Figure 95: View Unsupported Feature Warning Message.................................... 388
Figure 96: Install New Security Policies........................................................... 389
Figure 151: View Tokyo Routing Table for RB Site-to-Site VPN, MK ............... 493
Figure 152: Configure Paris Untrust Route for RB Site-to-Site VPN, MK .... 495
Figure 153: Configure Paris Trust Route for RB Site-to-Site VPN, MK ........ 495
Figure 154: Paris Routing Table for RB Site-to-Site VPN, MK .................. 496
Figure 155: Configure Rules for RB Site-to-Site VPN, MK ....................... 496
Figure 156: PB Site-to-Site VPN, MK Example Overview ......................... 497
Figure 157: Configure Two VPN Rules for PB Site-to-Site VPN, MK .......... 499
Figure 158: PB RAS VPN, L2TP Example Overview ............................... 500
Figure 159: Configure Rule for PB RAS VPN, L2TP ............................... 502
Figure 160: Central Manager UI and Regional Server UI ......................... 504
Figure 161: Single Sign-On ..................................................................... 505
Figure 162: Select Regional Servers ......................................................... 506
Figure 163: Add Regional Server ............................................................ 507
Figure 164: Add Regional Server ............................................................ 507
Figure 165: Link Regional Server Object to Central Manager Admin ............ 507
Figure 166: Deleting a Regional Server Object ...................................... 508
Figure 167: Log into a Regional Server .................................................... 509
Figure 168: NSM Opens Regional Server in a Separate Window ............... 510
Figure 169: Device Monitor Dialog Box .................................................. 517
Figure 170: View Device Detail Status ..................................................... 521
Figure 171: Device Statistics Bar Graph ................................................... 525
Figure 172: Protocol Distribution Dialog Box .......................................... 527
Figure 173: Process Status for IDP Sensor .............................................. 543
Figure 174: Device Statistics Summary for IDP Sensor ............................ 544
Figure 175: Monitoring VPNs ................................................................. 545
Figure 176: IDP Cluster Monitor ............................................................... 549
Figure 177: IDP Cluster Members ............................................................. 551
Figure 178: Server Monitor .................................................................... 554
Figure 179: Viewing Device Server Details ............................................. 556
Figure 180: Process Status for the Device Server .................................... 557
Figure 181: Process Status for the GUI Server ........................................ 557
Figure 182: Application Profiler View ..................................................... 568
Figure 183: Network Profiler View .......................................................... 569
Figure 184: Security Explorer ................................................................. 581
Figure 185: View Category and Severity Filters Messages ....................... 607
Figure 186: Log Viewer Navigation Controls .......................................... 608
Figure 187: Log Viewer Time Slider ....................................................... 609
Figure 188: Log Viewer Time Display ..................................................... 609
Figure 189: Viewing Summary Panel ...................................................... 619
Figure 190: Log Investigator UI Overview .............................................. 621
Figure 191: Configure Time Period Filter .............................................. 623
Figure 192: Changing Time Period Filter .............................................. 623
Figure 193: View Log Investigator Results ............................................. 627
Figure 194: Audit Log Viewer UI Overview ............................................ 631
Figure 195: Log Viewer Information for Top Information Logs Report ...... 666
Figure 196: Generating Quick Reports ................................................... 667
Figure 197: Select Log Viewer Flag ......................................................... 668
Figure 198: Logs by User-Set Flag Reports ............................................. 669
Figure 199: Top Rules Report Dialog Box .............................................. 670
Figure 200: FW/VPN Report ................................................................. 671
Figure 201: CIDR Translation ................................................................. 678
## List of Tables

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table 1</td>
<td>GUI Server Processes</td>
<td>14</td>
</tr>
<tr>
<td>Table 2</td>
<td>Device Server Processes</td>
<td>14</td>
</tr>
<tr>
<td>Table 3</td>
<td>Supported Security Devices</td>
<td>15</td>
</tr>
<tr>
<td>Table 4</td>
<td>Validation Status for Devices</td>
<td>23</td>
</tr>
<tr>
<td>Table 5</td>
<td>Validation Icons</td>
<td>24</td>
</tr>
<tr>
<td>Table 6</td>
<td>How to Authenticate Users</td>
<td>59</td>
</tr>
<tr>
<td>Table 8</td>
<td>Changes to “Edit Devices, Device Groups, &amp; Templates” Role</td>
<td>70</td>
</tr>
<tr>
<td>Table 9</td>
<td>Changes to View Devices, Device Groups, &amp; Templates Role</td>
<td>70</td>
</tr>
<tr>
<td>Table 10</td>
<td>Extended Bindings</td>
<td>90</td>
</tr>
<tr>
<td>Table 11</td>
<td>Security Device Port Mode Summary (Part 1)</td>
<td>91</td>
</tr>
<tr>
<td>Table 12</td>
<td>Security Device Port Mode Summary (Part 2)</td>
<td>91</td>
</tr>
<tr>
<td>Table 13</td>
<td>CSV File Information for Devices with Static IP Addresses</td>
<td>132</td>
</tr>
<tr>
<td>Table 14</td>
<td>CSV File Information for Devices with Dynamic IP Addresses</td>
<td>134</td>
</tr>
<tr>
<td>Table 15</td>
<td>CSV File Information for Undeployed Devices</td>
<td>135</td>
</tr>
<tr>
<td>Table 16</td>
<td>Delta Configuration Summary Information</td>
<td>182</td>
</tr>
<tr>
<td>Table 17</td>
<td>Device States During Update</td>
<td>191</td>
</tr>
<tr>
<td>Table 18</td>
<td>Scheduled Security Update (SSU) Command Line Parameters</td>
<td>205</td>
</tr>
<tr>
<td>Table 19</td>
<td>Deep Inspection Profile Actions</td>
<td>236</td>
</tr>
<tr>
<td>Table 20</td>
<td>Deep Inspection IP Actions</td>
<td>236</td>
</tr>
<tr>
<td>Table 21</td>
<td>IP Protocol Name and Type Numbers</td>
<td>246</td>
</tr>
<tr>
<td>Table 22</td>
<td>Supported Services for Service Bindings</td>
<td>247</td>
</tr>
<tr>
<td>Table 23</td>
<td>Attack Pattern Syntax</td>
<td>249</td>
</tr>
<tr>
<td>Table 24</td>
<td>Attack Pattern Syntax Example Matches</td>
<td>249</td>
</tr>
<tr>
<td>Table 25</td>
<td>DI Attack Header Match Modifiers</td>
<td>252</td>
</tr>
<tr>
<td>Table 26</td>
<td>Service Table Tab Information</td>
<td>282</td>
</tr>
<tr>
<td>Table 27</td>
<td>Group Expression Operators</td>
<td>305</td>
</tr>
<tr>
<td>Table 28</td>
<td>IDP Rule Actions</td>
<td>357</td>
</tr>
<tr>
<td>Table 30</td>
<td>Actions for Backdoor Rule</td>
<td>370</td>
</tr>
<tr>
<td>Table 31</td>
<td>Rule Shadowing Example</td>
<td>387</td>
</tr>
<tr>
<td>Table 32</td>
<td>Polymorphic Objects</td>
<td>408</td>
</tr>
<tr>
<td>Table 33</td>
<td>Device Status Information</td>
<td>518</td>
</tr>
<tr>
<td>Table 34</td>
<td>Device Polling Intervals</td>
<td>519</td>
</tr>
<tr>
<td>Table 35</td>
<td>Device Detail Status Items</td>
<td>521</td>
</tr>
<tr>
<td>Table 36</td>
<td>Device Statistics Summary</td>
<td>522</td>
</tr>
<tr>
<td>Table 37</td>
<td>Device Specific Views</td>
<td>523</td>
</tr>
<tr>
<td>Table 38</td>
<td>Policy Distribution Items</td>
<td>525</td>
</tr>
<tr>
<td>Table 39</td>
<td>Protocol Distribution Items</td>
<td>527</td>
</tr>
<tr>
<td>Table 40</td>
<td>VPN Monitor Table</td>
<td>529</td>
</tr>
<tr>
<td>Table 41</td>
<td>Active VPN Table</td>
<td>529</td>
</tr>
<tr>
<td>Table 42</td>
<td>Ethernet Statistics View Data</td>
<td>532</td>
</tr>
<tr>
<td>Table 43</td>
<td>Flow Statistics View Data</td>
<td>533</td>
</tr>
<tr>
<td>Table 44</td>
<td>Attack Counters</td>
<td>533</td>
</tr>
<tr>
<td>Table 45</td>
<td>Resource Statistics Items</td>
<td>536</td>
</tr>
<tr>
<td>Table 46</td>
<td>Administrators View</td>
<td>537</td>
</tr>
</tbody>
</table>
Table 47: Authenticated Users View .............................................................537
Table 48: Active Sessions Items .................................................................537
Table 49: HA Statistics View .....................................................................540
Table 50: Device Status Information .........................................................541
Table 51: IDP Device Detail Status Items ...................................................542
Table 52: IDP Sensor Process Status Items ................................................544
Table 53: Device Statistics Summary (for IDP Sensors) ...............................545
Table 54: VPN Tunnel Summary .................................................................546
Table 55: NSRP Device Summary ...............................................................547
Table 56: VSD/RTO Summary ...................................................................548
Table 57: VSD Counter Details ..................................................................548
Table 58: RTO Counters Details .................................................................549
Table 59: IDP Cluster Monitor ..................................................................550
Table 60: IDP Cluster Summary .................................................................550
Table 61: IDP Cluster Member Monitor .....................................................551
Table 62: Server Information .....................................................................552
Table 63: Server Monitor Data .................................................................554
Table 64: Server Detail Status .....................................................................556
Table 65: Process Status ...........................................................................558
Table 66: Management System Utilities ....................................................558
Table 67: General Profiler Settings ............................................................564
Table 68: Network Profiler Data ...............................................................568
Table 69: Network Profiler Data ...............................................................569
Table 70: Detailed Network Information Data ..........................................575
Table 71: Transitional Graphs ....................................................................585
Table 74: Destinations of Log Entry Severities .......................................592
Table 75: Self Log Entry Settings ...............................................................593
Table 76: Email Server Settings for Log Entries .......................................593
Table 77: Syslog Settings for Log Entries ..................................................600
Table 78: WebTrends Settings for Log Entries ..........................................601
Table 79: Log Categories ........................................................................603
Table 80: Log Viewer Columns ...............................................................604
Table 81: Search Tools for Log Viewer ....................................................608
Table 82: Log Viewer Flags ......................................................................611
Table 83: Irrelevant Vs. Relevant Attacks ..................................................620
Table 84: Log Investigator Filters .............................................................626
Table 85: Log Investigator Analysis .........................................................629
Table 87: Common Filters for Exporting Log Records .............................644
Table 88: Firewall and VPN Reports .........................................................654
Table 89: DI/IDP Reports ........................................................................654
Table 90: Screen Reports ..........................................................................655
Table 91: Administrative Reports .............................................................656
Table 92: UAC Reports ...........................................................................656
Table 93: Unmanaged Commands for Firewall/VPN Devices ..................695
Table 94: SurfControl Web categories ......................................................697
Table 95: Screen Alarm Log Entries .........................................................706
Table 96: Alarm Log Entries .....................................................................707
Table 97: Configuration Log Entries .........................................................774
Table 98: Information Log Entries ............................................................775
Table 99: Basic GTP Log Entry .................................................................777
Table 100: Extended GTP Log Entry .......................................................777
Table 101: Deleted GTP Tunnel Log Entry ................................................777
List of Examples

Using a Naming Convention for Security Devices ........................................... 47
Using a Naming Convention for Address Objects ........................................... 47
Configuring Role-Based Administration ....................................................... 72
User selects successfully update two devices with delta option .................... 121
User selects two devices to update with delta option and one device fails.... 121
User selects two devices to update without the delta option ........................ 121
User selects two devices to update with the delta option, but has no admin privileges .......................................................... 122
Adding a Vsys Cluster .................................................................................. 128
Using an Excel File to Add Multiple Static IP Devices ................................. 133
Using a Text File to Add Multiple Static IP Devices ..................................... 133
Using an Excel File to Add Multiple Dynamic IP Devices ............................ 134
Using a text File to Add Multiple Dynamic IP Devices ............................... 135
Using an Excel File to Add Multiple Modeled Devices ............................... 136
Using a text File to Add Multiple Modeled Devices .................................... 136
Configuring An Extranet Device .................................................................. 145
Creating a Device Template For DNS Settings .......................................... 152
Applying a Device Template ........................................................................ 153
Using Multiple Device Templates ................................................................. 159
Creating a Device Group ............................................................................. 165
Updating Devices With Different Attack Object Database Versions .......... 203
Confirm IDP Engine Version ........................................................................ 204
Update attack objects and push to connected devices .................................. 206
Using Cron Tab to Schedule Attack Updates ................................................. 207
Boolean Expression ...................................................................................... 258
CREATING A DYNAMIC GROUP .................................................................. 261
Configuring an External AV Profile ............................................................... 266
Creating a URL Custom list .......................................................................... 271
creating a Web Filtering Custom Profile ..................................................... 273
Viewing the predefined profile ..................................................................... 274
Creating a GTP Object .................................................................................. 280
Creating a Custom Service and Group .......................................................... 285
Creating a Custom Sun-rpc Service ............................................................... 286
Creating a Custom MS-rpc Service ................................................................. 287
Replacing HTTP with HTTPS ....................................................................... 288
Configuring a RADIUS Auth Server .............................................................. 294
Using RADIUS with User Groups ................................................................. 300
Configuring an IP Pool Object ...................................................................... 304
Creating a Group Expression ....................................................................... 306
Configuring An Extranet Policy object ......................................................... 312
Creating a standalone IDP security policy .................................................... 329
Setting Individual Sources and Destinations in rules .................................. 332
NetScreen-Security Manager 2007.2 Administrator's Guide

Setting Group Sources and Destinations in rules .............................................332
Negating Sources in rules ..............................................................................333
Setting Standard Services in rules .................................................................333
Setting Custom Services in rules .................................................................334
Setting Schedule Objects in rules .................................................................340
Setting a WEB Filtering Profile in a Rule .......................................................342
Creating a Multicast Rule ............................................................................348
Setting Source and Destination ..................................................................352
Setting Multiple Sources and Destinations ....................................................352
Setting Default Services .............................................................................353
Setting Custom services .............................................................................353
Setting Non-Standard Services ...................................................................354
Setting Terminal Rules .................................................................................355
Configuring Rules for an ISG in standalone idp mode ..................................363
Exempting a Source/Destination Pair ...........................................................365
Exempting Specific Attack Objects ...............................................................366
Using Zone Exceptions .................................................................................392
Merging Security Policies .............................................................................397
Exporting Zone based Firewall rules with expanded view .........................399
Configuring an AutoKey IKE, Policy-Based Site-to-Site VPN ......................452
Configuring an AutoKey IKE RAS, Policy-Based VPN ..................................457
Configuring an AutoKey IKE, Route-Based Site-to-Site VPN .......................461
Configuring XAuth Authentication with External User Group .....................468
Configuring a Route-Based Site-to-Site VPN, Manual Key .........................489
Configuring a Policy-Based Site-to-Site VPN, Manual Key .........................496
Configuring a Policy-Based RAS VPN, L2TP .............................................500
Monitoring Device Status ............................................................................551
Tailing incoming Logs in the Log Viewer ......................................................610
Using Filters in the log Viewer ....................................................................614
Customizing Log Viewer Columns ..............................................................617
Setting a Time Interval in the Log Investigator ............................................623
Using Left and Top Axes in the Log Investigator ..........................................624
Setting Filters in the Log Investigator ..........................................................627
Viewing Destination Ports in the Log Investigator ........................................629
Viewing Subcategory Details in the Log Investigator ....................................630
Viewing Time Period in the log investigator ................................................630
Exporting Attack Category Log Records to XML ........................................646
Exporting Column Headers to CSV .............................................................646
Exporting to a SNMP Server ......................................................................647
Creating a Custom Report ..........................................................................658
Using Cron Tab to Schedule Attack Updates .................................................661
Using Administrative Reports to Track Incidents ........................................667
Using Administrative Reports to Optimize Rulebases ..................................669
Using FW/VPN Report to Track Configuration Changes ..............................670
Using Screen Reports to Identify Attack Trends ..........................................671
Using DI Reports to Detect Application Attacks ...........................................671
About This Guide

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

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

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

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

This chapter contains the following sections:

- Audience on page xxxii
- Conventions on page xxxii
- Documentation on page xxxiv
- Contacting Customer Support on page xxxvii
Audience

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

Conventions

This document uses the conventions detailed in the following sections.

User Interface Conventions

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

Figure 1: UI Navigation Example

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

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

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

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

**Figure 2: Graphic Conventions**

- Local Area Network (LAN) with a Single Subnet, (example: 10.1.1.0/24)
- Security Zone Interfaces
  - White = Protected Zone Interface (example: Trust Zone)
  - Black = Outside Zone Interface (example: Untrust Zone)
- Security Device
- Desktop Computer
- Laptop Computer
- Server
- VPN Tunnel
- Router
- Switch
- Tunnel Interface
- Internet
- Internet

**Unsupported Characters**

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

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

---

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

- Number sign ( # )
- Dollar sign ( $ )
- Percent sign ( % )
- Circumflex ( ^ )
- Ampersand ( & )
- Asterisk ( * )
- Square brackets ( [ ] )
- Curly brackets ( { } )
- Parentheses ( ( ) )
- Forward slash ( / )
- Greater than sign ( > )
- Single straight quote ( ' )
- Single curly quote ( ' )
- Period ( . )

Documentation

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

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

NetScreen-Security Manager Administrator’s Guide

The following sections detail each chapter in the NetScreen-Security Manager Administrator’s Guide.
Part 1: Preparing

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

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

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

Part 2: Integrating

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

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

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

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

Part 3: Managing

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


Chapter 10 “Configuring VPNs” provides an overview on 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.

Chapter 11 “Central Manager” details how to set up and use Central Manager.

Part 4: Monitoring

Chapter 12 “Realtime Monitoring” details the firewall, VPN, and NSRP monitoring functionality of NetScreen-Security Manager.
Chapter 13 “Analyzing Your Network” details how to use the Profiler as a network-analysis tool that helps you learn about your internal network, enabling you to create effective Security Policies and minimize unnecessary log records.

Chapter 14 “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 15 “Reporting” details how to create reports from log information.

Part 5: Appendixes
Appendix A, Glossary defines terms and concepts used in the NetScreen-Security Manager environment.

Appendix B, Unmanaged ScreenOS Commands details unsupported ScreenOS CLI commands.

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

Appendix D, Common Criteria EAL2 Compliance details EAL2 common criteria for IDP-capable security devices.

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

Part 6: Index
The index provides an alphabetical list of the major topics and subtopics discussed in this document, and their corresponding page numbers.

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

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

NetScreen-Security Manager: Configuring Firewall/VPN Devices
This guide details how to create a device configuration, including zones, interfaces, and routes. It also 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.
NetScreen-Security Manager Online Help
The online help provides task-oriented procedures that describe how to perform basic tasks in the NetScreen-Security Manager user interface. It also includes a brief overview of the NetScreen-Security Manager system and a description of the GUI elements.

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

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

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

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

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

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

- techpubs-comments@juniper.net

Along with your comments, be sure to indicate:

- Document name
- Document part number
- Page number
- Software release version

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

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

Part 1 contains the following chapters:

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

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

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

After you have become familiar with NetScreen-Security Manager features and the UI, and you have designed a domain structure and administrator roles that meet the architectural and security needs of your network (or networks), you are ready to begin the process of integration, as detailed in Part 2, “Integrating” on page 77.
Chapter 1

Introduction to NetScreen-Security Manager

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

This chapter contains the following sections:

- About NetScreen-Security Manager on page 4
- Technical Overview on page 11
- Working in the User Interface on page 17
- New Features in NetScreen-Security Manager 2007.2 on page 29
About NetScreen-Security Manager

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

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

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

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

Security Integration

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

Complete Support

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

Network Organization

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

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

**Role-Based Administration**

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

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

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

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

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

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

**NOTE:** In a mixed environment, an Administrator with the IDP Administrator role is unable to take full command of a firewall device because of the predefined restrictions. If an IDP Administrator is expected to manage a firewall device in a mixed environment, they should be alerted to the restrictions and have their role(s) modified to include the necessary permissions.

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

• **Shared Objects**—An object is a NetScreen-Security Manager definition that is valid in the global domain and all subdomains. Any object created in the global domain is a shared object that is shared by all subdomains; the subdomain automatically inherits any shared objects defined in the global domain. You will not see global objects in the Object Manager of a subdomain, however, you can use the objects when selecting objects in a policy.

The global domain is a good location for security devices and systems that are used throughout your organization, address book entries for commonly used network components, or other frequently used objects. A subdomain, alternatively, enables you to separate firewalls, systems, and address objects from the global domain and other subdomains, creating a private area to which you can restrict access.

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

**Migration Tools**

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

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

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

**Device Management**

A production network is a living entity, constantly evolving to adapt to the needs of your organization. As your network grows, you might need to add new devices, reconfigure existing devices, update software versions on older devices, or integrate a new network to work with your existing network. NetScreen-Security Manager helps you take control of your network by providing a virtual environment in which to first model, verify, then updated your managed devices with changes.
Device Modeling
Using your virtual network to change, review, and test your network configuration before deploying it to your physical network can help you discover problems like routing issues, IP conflicts, and version mismatches across your entire network before they actually occur. NetScreen-Security Manager includes configuration validation to help you identify device configuration errors and missing information, then points you to the trouble spot so you can quickly fix the problem. When you have designed a virtual configuration that works, you can push this configuration to your devices with a single update.

With NetScreen-Security Manager, you can implement a new routing protocol across your network, design and deploy a new Security Policy with traffic shaping, or create a new VPN tunnel that connects a branch office to your corporate network—then deploy all changes with a single click.

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

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

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

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

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

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

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

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

- **Security and Protection**—Configure a rule to look for attacks, viruses, or specific URLs (devices running ScreenOS 5.x and higher).
- **Traffic Shaping**—Use your firewall rules to control the amount of traffic permitted through your security devices.

### Error Prevention, Recovery, and Auditing

Persistent management control is essential when managing large networks. You need to be sure that configuration and policies you send to your managed devices are correct before you install them on your devices.

Using NetScreen-Security Manager’s error prevention and recovery features, you can ensure that you are consistently sending stable configurations to your devices, and that your device remained connected to NetScreen-Security Manager. Additionally, you can track each change made by a NetScreen-Security Manager administrator to help you identify when, how, and what changes were made to your managed devices.

### Device Configuration Validation

NetScreen-Security Manager automatically alerts you to configuration errors while you work in the UI. Each field that has incorrect or incomplete data displays a warning icon—move your mouse cursor over the icon to get details on the missing data. For more details on validation, see “Validation Icons in the User Interface” on page 23.

### Policy Validation

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

### Atomic Configuration and Updating

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

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

### Device Image Updates

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

- **NetScreen-Security Manager updates**—Use NetScreen-Security Manager to upload the new image file to multiple security devices with a single click.
RMA updates—To replace failed devices, set the device to the RMA state, which enables NetScreen-Security Manager to retain the device configuration without a serial number or connection statistics. When you install the replacement device, activate the device with the serial number of the replacement unit.

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

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

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

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

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

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

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

- **Dynamic, route-based VPNs**—Provide resilient, always-on access across your network. Add firewall rules on top of a route-based VPNs to control traffic flow.
- **Policy-based VPNs**—Connect devices, remote access service (RAS) users, and control traffic flow (can also create with L2TP).
Mixed-mode VPNs—Connect route-based VPNs with policy-based VPNs, giving you flexibility.

Integrated Logging and Reporting
You use the security devices on your network for multiple reasons: to control access to and from your network, to detect and prevent unwanted intruders, and to record security events so you can monitor the important activities occurring on your network. You can use NetScreen-Security Manager to monitor, log, and report on network activity in real-time to help you understand what is happening on your network:

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

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

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

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

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

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

**Technical Overview**

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

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

**Architecture**

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

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

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

When using Central Manage, its installer will install the Central Manager GUI Server and will present you with minimum choices with regard to configuration. The installer supports GuiSvr, extended HA support and statistical report server.

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

Management System

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

The management system itself is composed of two distinct components:

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

![NetScreen-Security Manager System Architecture](image)

**GUI Server**

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

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

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

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

Table 1 describes the processes that the GUI Server runs when you start this server.
Table 1: GUI Server Processes

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

Table 2 describes the processes that the Device Server runs when you start this server:

Table 2: Device Server Processes

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

Table 3 details the security devices and firmware versions supported by NetScreen-Security Manager:

<table>
<thead>
<tr>
<th>Managed Device</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>devSvrDBServer</td>
<td>Device Server Database Server</td>
</tr>
<tr>
<td>devSvrProfilerMgr</td>
<td>Device Server Profiler Manager</td>
</tr>
</tbody>
</table>

### Table 3: Supported Security Devices

<table>
<thead>
<tr>
<th>Security Device</th>
<th>Firmware Versions Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>Juniper Networks NetScreen-5XP</td>
<td>ScreenOS 4.0.0, 4.0.1, 4.0.3, 5.0, 5.0 FIPS</td>
</tr>
<tr>
<td>Juniper Networks NetScreen-5XT</td>
<td>ScreenOS 4.0.0, 4.0.1MCAST, 4.0.3, 5.0, 5.1, 5.2, 5.3</td>
</tr>
<tr>
<td>Juniper Networks NetScreen-5GT</td>
<td>ScreenOS 4.0.0-DIAL2, 5.0, 5.0DIAL, 5.0FIPS, 5.1, 5.2, 5.3</td>
</tr>
<tr>
<td>Juniper Networks NetScreen-5GT ADSL</td>
<td>ScreenOS 5.0ADSL, 5.2, 5.3</td>
</tr>
<tr>
<td>Juniper Networks NetScreen-5GT WLAN</td>
<td>ScreenOS 5.0WLAN, 5.3</td>
</tr>
<tr>
<td>Juniper Networks NetScreen-HSC</td>
<td>ScreenOS 5.0, 5.0FIPS, 5.1, 5.2, 5.3</td>
</tr>
<tr>
<td>Juniper Networks NetScreen-25</td>
<td>ScreenOS 4.0.0, 4.0.1, 4.0.1MCAST, 4.0.3, 5.0, 5.0FIPS, 5.1, 5.2, 5.3</td>
</tr>
<tr>
<td>Juniper Networks NetScreen-50</td>
<td>ScreenOS 4.0.0, 4.0.1, 4.0.1IGMP, 4.0.1MCAST, 4.0.3, 5.0, 5.0FIPS, 5.1, 5.2, 5.3</td>
</tr>
<tr>
<td>Juniper Networks NetScreen-100</td>
<td>ScreenOS 4.0.0</td>
</tr>
<tr>
<td>Juniper Networks NetScreen-204</td>
<td>ScreenOS 4.0.0, 4.0.1, 4.0.1MCAST, 4.0.3, 5.0, 5.0FIPS, 5.1, 5.2, 5.3</td>
</tr>
<tr>
<td>Juniper Networks NetScreen-208</td>
<td>ScreenOS 4.0.0, 4.0.1, 4.0.1MCAST, 4.0.3, 5.0, 5.0FIPS, 5.1, 5.2, 5.3</td>
</tr>
<tr>
<td>Juniper Networks NetScreen-500</td>
<td>ScreenOS 4.0.0, 4.0.1, 4.0.1MCAST, 4.0.3, 5.0, 5.0FIPS, 5.0NSGP, 5.0GPRS, 5.1, 5.1GPRS, 5.2, 5.3</td>
</tr>
<tr>
<td>Juniper Networks NetScreen-5200/8</td>
<td>ScreenOS 4.0.0, 4.0.1, 4.0.1IGMP, 4.0.1MCAST, 4.0.1SBR, 4.0.1SIBR, 4.0.3, 5.0, 5.0FIPS, 5.0NSGP, 5.0L2V, 5.1, 5.2, 5.3</td>
</tr>
<tr>
<td>Juniper Networks NetScreen-5400</td>
<td>ScreenOS 4.0.1-SBR, 4.0.1-SIBR, 5.0, 5.0NSGP, 5.1, 5.2, 5.3</td>
</tr>
<tr>
<td>Juniper Networks ISG-1000</td>
<td>ScreenOS 5.0, 5.0IDP1, 5.3</td>
</tr>
<tr>
<td>Juniper Networks ISG-2000</td>
<td>ScreenOS 5.0, 5.0FIPS, 5.0IDP1, 5.2, 5.3</td>
</tr>
<tr>
<td>Juniper Networks SSG-5</td>
<td>ScreenOS 5.4 and higher</td>
</tr>
<tr>
<td>Juniper Networks SSG-20</td>
<td>ScreenOS 5.4 and higher</td>
</tr>
<tr>
<td>Juniper Networks SSG-140</td>
<td>ScreenOS 5.4 and higher</td>
</tr>
<tr>
<td>Juniper Networks SSG-520</td>
<td>ScreenOS 5.1, 5.4</td>
</tr>
<tr>
<td>Juniper Networks SSG-550</td>
<td>ScreenOS 5.1, 5.4</td>
</tr>
</tbody>
</table>
Distributed Data Collection

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

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

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

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

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

Security

NetScreen-Security Manager integrates application-level encryption and authentication and uses high-grade encryption and public-key algorithms to eliminate the need for separate IPSEC tunnels between each device and the management station.
For communication between the UI, the GUI Server, and the Device Server, NetScreen-Security Manager uses Secure Server Protocol (SSP), a modified version of TCP that is more reliable than ordinary TCP, requires less CPU and memory resources from servers, and reduces the number of acknowledgement packets on the network. SSP uses AES encryption and SHA1 authentication for all connections.

Scaling and Performance

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

Working in the User Interface

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

Characters Not Supported in Login Passwords

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

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

NOTE: Passwords in the NetScreen-Security Manager UI are case-sensitive.

Managing Blocked Login Attempts

The NetScreen-Security Manager UI blocks hosts that attempt to login and fail after ten tries by default. Use the Tools > Preferences > System Properties option to change this behavior. Use the Tools > Manage Blocked Hosts option to unblock hosts that have been locked out of the UI due to excessive failed login attempts.
Configuring UI Preferences

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

UI Overview

The NetScreen-Security Manager User Interface (UI) appears after you log in, and displays a set of menus and toolbar icons at the top of the UI window. Depending on the component displayed, right-click menus are available to perform various tasks. The UI is shown below:

Figure 3: Overview of the User Interface

Navigation Tree

The navigation tree displays the 11 NetScreen-Security Manager modules in the left pane of the NetScreen-Security Manager window. Double-click a module to display its contents in a hierarchical tree format. For details about each module, see “NetScreen-Security Manager Modules” on this page.

Main Display Area

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

- **Menu Bar**—The menu bar contains clickable commands. You can access many menu bar commands using keyboard shortcuts such as add, edit, delete. For a complete list of keyboards shortcuts, see the NetScreen-Security Manager Online Help.

- **ToolBar**—The toolbar contains buttons for common tasks. The buttons displayed in the toolbar are determined by the selected module.
- **Status Bar**—The status bar displays additional information for a selected module.

**NetScreen-Security Manager Modules**

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

**Log Viewer**

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

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

Use the Log Viewer to:

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

For more details on using the Log Viewer, see Chapter 14, "Logging".

**Report Manager**

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

**Log Investigator**

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

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

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

- **Security devices and systems**—The devices you use to enable access to your network and to protect your network against malicious traffic.

- **Vsys devices**—A vsys is a virtual device that exists within a physical security device.

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

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

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

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

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

Security Policies

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

Use Security Policies to:

- Add or modify existing Security Policies

- Add or modify existing VPN rules

- Add or modify existing IDP rules

- Create new policies based on existing policies

- Install policies on one or multiple security devices

- Delete policies

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

VPN Manager

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

- Define the protected resources on your network. Protected Resources represent the network resources you want to protect in a VPN.
- Create custom IKE Phase 1 and 2 Proposals.
- Configure AutoKey IKE, L2TP, and L2TP-over-AutoKey IKE VPNs in policy-based or route-based modes. You can also create an AutoKey IKE mixed mode VPN to connect policy-based VPN members with route-based VPNs members.
- Configure AutoKey IKE and L2TP policy-based VPNs for remote access services (RAS) and include multiple users.

Object Manager

The Object Manager contains objects, which are re-usable, basic NetScreen-Security Manager building blocks that contain specific information. You use objects to create device configurations, policies, and VPNs. All objects are shared, meaning they can be shared by all devices and policies in the domain.

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

- **Address Objects**—Represent components of your network (hosts, networks, servers).
- **Schedule Objects**—Represent specific dates and times. You can use schedule objects in firewall rules to specify a time or time period that the rule is in effect.
- **DI Profiles**—Define the attack signature patterns, protocol anomalies, and the action you want a security device to take against matching traffic.
- **IDP Attack Objects**—Attack patterns that detect known and unknown attacks. You use IDP attack objects within IDP rules.
- **AV Objects**—Represent the AV servers, software, and profiles available to devices managed by NSM.
- **ICAP Objects**—Represents the Internet Content Adaptation Protocol (ICAP) servers and server groups used in ICAP AV objects.
- **Web Filtering Objects** (Web Profiles)—Define the URLs, the Web categories, and the action you want a security device to take against matching traffic.
- **Service Objects**—Represent services running on your network, such as FTP, HTTP, and Telnet. NetScreen-Security Manager contains a database of Service Objects for well-known services; you can also create new Service Objects to represent the custom services you are running on your network.
- **User Objects**—Represent the remote users that access the network protected by the security device. To provide remote users with access, create a user object for each user, then create a VPN that includes those user objects.
- **IP Pools**—Represent a range of IP addresses. You use IP pools when you configure a DHCP Server for your managed devices.
- **Authentication Servers**—Represent external authentication servers, such as RADIUS and SecurID servers. You can use an authentication server object to authenticate NetScreen-Security Manager admins (RADIUS only), XAuth users, IKE RAS users, and L2TP users.

- **Group Expressions**—Are OR, AND, and NOT statements that set conditions for authentication requirements.

- **Remote Settings**—Represent DNS and WINS servers. You use remote settings object when configuring XAuth or L2TP authentication in a VPN.

- **NAT Objects**—Represent MIPs, VIPs, and DIPs.

- **GTP Objects**—Represent GTP client connections.

- **CA Objects**—Represent the certificate authority’s certificate.

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

You can use the Object Manager to:

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

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

**Server Manager**

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

**Realtime Monitor**

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

- **Device Monitor**—Tracks the connection state and configuration state of your security devices and IDP sensors. 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 security devices in clusters.

- **IDP Cluster Monitor**—Tracks the status of IDP clusters.

You can customize Realtime Monitor to display only the information you want to see, as well as update information at specified time periods. You can also set alarm criteria for a device or process. For more details on Realtime Monitor, see Chapter 12, “Realtime Monitoring”.
Security Monitor

Security Monitor provides access to the Dashboard, Profiler and Security Explorer. These tools enable you to track, correlate and visualize aspects about your internal network, enabling you to create more effective Security Policies and minimize unnecessary log records. For more details, refer to “Analyzing Your Network” on page 561.

Job Manager

Job Manager contains the status of commands (also called directives) that NetScreen-Security Manager sends to your managed devices. You can view summaries or details for active jobs and completed jobs. For more details on Job Manager, refer to “Tracking Device Updates” on page 188.

Audit Log Viewer

The Audit Log Viewer contains a log entry for every change made by a NetScreen-Security Manager administrator. For more details on Audit Log Viewer, see “Using the Audit Log Viewer” on page 631.

Action Manager

The Action Manager enables you to forward logs on a per domain basis. For more details on using the Action Manager, refer to “Using the Action Manager to Forward Logs by Domain” on page 640.

Validation Icons in the User Interface

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

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

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

Table 5: Validation Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Message Type</th>
<th>Meaning</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Error icon]</td>
<td>Error</td>
<td>Indicates that a configuration or parameter is not configured correctly in the NetScreen-Security Manager UI. Updating a device with this modeled configuration causes problems on the device.</td>
<td>Highest</td>
</tr>
<tr>
<td>![Warning icon]</td>
<td>Warning</td>
<td>Indicates that a configuration or parameter is not configured correctly in the NetScreen-Security Manager UI. Updating a device with this modeled configuration might cause problems on the device.</td>
<td></td>
</tr>
<tr>
<td>![Override icon]</td>
<td>Override</td>
<td>Indicates that the displayed value was set manually and that the value overrides whatever value might come from a template. The icon can also indicate an override of a VPN-provided value or a cluster-provide value.</td>
<td></td>
</tr>
<tr>
<td>![Template Value icon]</td>
<td>Template Value</td>
<td>Indicates that the displayed value was set manually. Changes to the same field in the template will be applied to the device when it is updated.</td>
<td></td>
</tr>
<tr>
<td>![From Object icon]</td>
<td>From Object</td>
<td>Indicates that the displayed value came from the device when the device was imported. Changes to a template will not change this value unless “Remove conflicted device values” is selected in the template Operations dialog.</td>
<td>Lowest</td>
</tr>
</tbody>
</table>

From Object messages only appear when viewing template objects to help find fields set in the template.

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

Working with Other NetScreen-Security Manager Administrators

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

- When an NetScreen-Security Manager admin begins editing an object, the UI locks that object to prevent other admins from editing the object’s value.
- During lockout, NetScreen-Security Manager makes “lazy” saves of all edits made and stores them in an in-memory database. If NetScreen-Security Manager crashes during a lazy save, edits made since the last lazy save are lost, and NetScreen-Security Manager prompts the NetScreen-Security Manager admin to rollback to the last lazy save.
When the admin completes and saves the edit, that object is unlocked, enabling other admins to edit it. However, because the UI does not immediately refresh the object values, you must manually refresh the UI to view the most recent versions.

When you attempt to open a locked object, a warning message appears indicating that the object is locked and can be opened only as a read-only object. The warning message also contains the name of the NetScreen-Security Manager administrator that is currently editing the object. Depending on your administrator privileges, you can locate contact information for the admin in the Manage Administrators and Domains area of the UI (From the file menu, select Tools > Manage Administrators and Domains). For details on working with administrators and domains, see “Configuring Role-Based Administration” on page 57.

For example, let’s say Bob and Carol are both NetScreen-Security Manager admins with the same roles. If both admins view the same object, but Bob also edits and saves the object, NetScreen-Security Manager does not notify Carol that a newer version of the object exists. To see the newest version, Carol must first close, then open the object again or refresh the console.

### Searching in the User Interface

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

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

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

![UI Search Modes](image)

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

**Contains String [C] Search Mode**

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

1. In the main navigation tree, select **Object Manager > Service Objects > Predefined Service Objects**, then select the Service Object icon at the top of the **Service Tree** tab.
2. Press the backslash key (\) to display the search mode window.

3. Enter C, then enter RPC. The UI automatically highlights the first match, MS-RPC-ANY, as shown below.

Figure 5: "Contains String" Search Mode Example

Starts With [S] Search Mode
Use to locate a pattern at the beginning of a string. For example, to locate the pattern "OR" in security devices:

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

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

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

Figure 6: "Starts With" Search Mode Example

Regular Expression [R] Search Mode
Use to locate a value using a regular expression. For example, to locate all attack objects that detect denial-of-service attacks:
1. In the main navigation tree, select **Object Manager > Attack Objects**, then select the **Predefined Attacks** tab.

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

3. Enter **R**, then enter the following characters: **Do$|enial**. The following figure details this expression:

   Figure 7: “Regular Expression” Search Mode Details

   The pipe character (|) represents an OR relationship.

   The period character (.) represents any character. In this example, you are searching for word “denial” or “Denial”.

   “DoS” is a common acronym for denial-of-service.

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

   Figure 8: “Regular Expression” Search Mode Example

<table>
<thead>
<tr>
<th>Predefined Attacks</th>
<th>Predefined Attack Group</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Match 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>{R}</code>: “Do$</td>
<td>enial”</td>
</tr>
<tr>
<td>SMB Error: Invalid Message Length</td>
<td></td>
</tr>
<tr>
<td>SMB Error: Malformed Message</td>
<td></td>
</tr>
<tr>
<td>DOS Network Device: 3Com OfficeConnect HTTP Router Denial of Service</td>
<td></td>
</tr>
<tr>
<td>CSCO IOS Httpd DoS</td>
<td></td>
</tr>
<tr>
<td>FTP: Line Too Long</td>
<td></td>
</tr>
<tr>
<td>FTP: Password Too Long</td>
<td></td>
</tr>
<tr>
<td><strong>Match 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>{R}</code>: “Do$</td>
<td>denial”</td>
</tr>
<tr>
<td>SMB Error: Invalid Message Length</td>
<td></td>
</tr>
<tr>
<td>SMB Error: Malformed Message</td>
<td></td>
</tr>
<tr>
<td>DOS Network Device: 3Com OfficeConnect HTTP Router Denial of Service</td>
<td></td>
</tr>
<tr>
<td>CSCO IOS Httpd DoS</td>
<td></td>
</tr>
<tr>
<td>FTP: Line Too Long</td>
<td></td>
</tr>
<tr>
<td>FTP: Password Too Long</td>
<td></td>
</tr>
</tbody>
</table>

**NOTE:** The regular expression search mode supports all common regular expressions. For more information about regular expressions, refer to a dedicated resource, such as *Mastering Regular Expressions*, 2nd Edition, by Jeffrey E. F. Friedl.
IP [I] Search Mode

Use to locate an IP address. For example, to locate the IP address 5.5.5.50 and 5.5.5.51 in Address Objects:

1. In the main navigation tree, select Object Manager > Address Objects, then select the Address Table tab.

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

3. Enter I, then enter 5.5.5.*. The UI automatically highlights the first match, **5.5.5.50**. Click the down arrow key to highlight the next match, **5.5.5.51**.

When searching in a table, your search criteria is applied only to the selected column. If you select a different column, such as Name, and perform the same search, your results differ. Figure 8 shows both search results.

Figure 9: “IP Address” Search Mode Example

![Table of Address Objects]

New Features in NetScreen-Security Manager 2007.2

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

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

The following is a list of new features and enhancements in this NSM release:

- **Central Manager**—Features of the Central Manager include:
  - **Management of Regional Servers**—The primary function of your Central Manager will be the management of Regional Servers. From the Central Manager you will be able to add, delete and manage Regional Servers.
  - **Global Pre/Post Rules**—In NSM, a policy supports many kinds of rulebases. Each rulebase is an ordered list of rules. Pre-rules and Post-rule are two ordered lists of rules, which are defined on the Central Manager as part of a policy and pushed to the desired Regional Servers (Global Policy Install).
  - **Polymorphic Objects**—Pre/Post Rules defined on the Central Manager may use some shared objects where one or more fields may be defined in the context of the Regional Server to which the rules will be pushed. To provide the regional server admin the capability of customizing Central Manager pre/post rules to their specific environment, the concept of Polymorphic Objects has been established. In Central Manager, the following objects categories can have a polymorphic type: Address, Service and Zone.

- **Regional Server**—Features of the Regional Server include:
  - **Pre-and-Post Domain Rules**—A Domain Administrator can specify a policy definition at a domain level that will apply to all devices within the specific domain and all subdomains. The rules can be applied as pre and post rules for any device in the given domain and subdomains.
  - **High Availability (HA) Enhancements**—These enhancements includes:
    - Improved database synchronization by utilizing database replication feature of Berkeley Database
    - Support for HA server running as a non-root process
    - Additional parameters to make HA control more configurable
    - Enhanced HA notification and logging mechanism.
  - **Identity-Enabled Profiler**—This feature correlates UAC logs (user information) with Profiler Data (application information). It is available for use with ISG devices running ScreenOS 5.4R2 with IDP configurations or ScreenOS 6.0 with IDP configurations. This feature provides administrators a view of what applications are being used at the user level.
  - **NSM Information Banner after Login**—Optional server-wide setting that allows the super administrator to create custom text that is shown on an information banner after login credentials are accepted by the NSM Server.
- **Job Manager Usability Enhancements**—The admin name associated with a submitted job will be now be displayed in the Job Manager to improve usability.

**NSM Xpress Appliance**

NSM Xpress is an appliance version of NetScreen-Security Manager. It installs in minutes with full support for High Availability (HA), making it easy to scale and deploy. This fully-integrated appliance provides out of the box installation and Management of NSM. You can configure your NSM Xpress to be a Central Manager (CM) of Regional Server(s).
Security devices are the Juniper Networks security components that you use to enable access to your network components and to protect your network against malicious traffic. When you use NetScreen-Security Manager to manage your security devices, you are creating a virtual network that represents your physical network. Using this virtual network, you can create, control, and maintain the security of your physical network at a system-level.

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

This chapter contains the following sections:

- Configuring Security Devices Overview on page 32
- Configuring IDP-Capable Devices Overview on page 35
- Simplifying Management on page 45
- Creating an Information Banner on page 48

NOTE: Not all devices support all features described in this guide. For device-specific datasheets that include an updated feature list for each device, go to: http://www.juniper.net/products/integrated/dsheet/. This link is provided for your convenience and may change without notice. You can also find these information by going to the Juniper web site (http://www.juniper.net/).
Configuring Security Devices Overview

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

NOTE: Juniper Networks also offers security devices with Instruction Detection and Prevention (IDP) capability. For details on how to enable IDP functionality on these devices, see “Configuring IDP-Capable Devices Overview” on page 35.

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

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

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

Importing Existing Devices

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

To import and configure your existing devices:

1. Add the security device and import your device configuration.
   a. In the NetScreen-Security Manager main navigation tree, select Device Manager > Security Devices.
   b. In the main display area, click the Add icon and select Add Device. Follow the instructions in the Add Device Wizard to import the security device.

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

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

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

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

### Modeling New Devices

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

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

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

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

3. Add your security devices and create their device configurations. You’ll need to define zones, assign interfaces, and designate virtual routers to enable the firewall to pass traffic on the network.
   - Use templates to configure multiple devices. Templates help you re-use common information to quickly create configurations for similar devices.
For ScreenOS 5.x devices, you can use Rapid Deployment (RD) to deploy multiple devices in non-technical locations. Use RD to stage and configure devices quickly, then simultaneously update all device with policies to control traffic as desired in multiple locations.

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

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

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

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

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

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

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

Common Criteria EAL2 Compliance

All Juniper Networks IDP Sensors are designed to meet the Common Criteria requirements for Common Criteria EAL2. This section describes actions that are required for a security administrator to properly secure the NetScreen-Security Manager system and NetScreen-Security Manager User Interface to be in compliance with the Common Criteria EAL2 security target for Juniper Networks NetScreen-IDP 4.x.

The NetScreen-Security Manager system consists of the Device Server and the GUI Server; the NetScreen-Security Manager User Interface is a client application used to access information stored in the NetScreen-Security Manager system.

Guidance for Intended Usage

The NetScreen-Security Manager system must be installed on dedicated systems. These dedicated systems must not contain user processes that are not required to operate the NetScreen-Security Manager software.

Guidance for Personnel

The following items are also required for Common Criteria EAL2 compliance:

- There must be one or more competent individuals assigned to manage the NetScreen-Security Manager system and User Interface, and the security of the information that they contain.

- The authorized administrators must not be careless, willfully negligent, or hostile and must follow and abide by the instructions provided by the NetScreen-Security Manager documentation.

- The NetScreen-Security Manager system and User Interface must be accessed only by authorized users.
Guidance for Physical Protection

The processing resources of the NetScreen-Security Manager system and User Interface must be located within facilities with controlled access which prevents unauthorized physical access.

Supported IDP-Capable Devices

NetScreen-Security Manager supports IDP on standalone IDP Sensors (IDP 10, 50, 100, 200, 500, 600, 1000, and 1100) and as part of ISG 2000 and ISG 1000 security systems running ScreenOS 5.0.0-IDP1 and ScreenOS 5.4 and higher.

Standalone IDP Sensors

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

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

NOTE: IDP Sensors are standalone appliances that provide IDP functionality without integrated FW/VPN capabilities.

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

Enabling IDP Functionality

To enable IDP functionality on the security device and deploy that functionality to protect your network, you must perform the steps listed below, which are detailed in the following sections.

- Adding ISG 2000/ISG 1000 Security Device with Security Module on page 37
- Installing Advanced License Keys on page 37
- Updating Attack Objects on page 37
- Adding Objects (Optional) on page 38
- Configuring a Security Policy for IDP on page 38
Adding ISG 2000/ ISG 1000 Security Device with Security Module
You must add an ISG 2000 or ISG 1000 security device with at least one security module to the NetScreen-Security Manager UI before you can enable the IDP functionality in security module.

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

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

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

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

Installing Advanced License Keys
To access the IDP functionality on a security module, you must install both an Advanced license key and an IDP license key on the security device. For details on obtaining and installing a license key, see “Managing License Keys” on page 196.

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

Updating Attack Objects
You must update the attack object database before you can use IDP functionality. To update the IDP and DI databases and the IDP detector engine, download new attack objects from the attack object database server to the GUI Server.

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

To update the IDP and DI attack object databases on the NetScreen-Security Manager GUI Server:

1. Select **Tools > Update NSM Attack Database** to open the **Update NSM Attack Database** dialog.
2. Follow the instructions in the Attack Update Manager to download the new Signature and Protocol Anomaly Attack Objects to the NetScreen-Security Manager GUI Server. The management system contacts the server and downloads the latest database version to the GUI Server.
After you have updated the attack object database on the GUI Server, you can use that database to update the attack object database on your managed devices.

IDP attack objects are loaded onto IDP-capable devices with the IDP rulebase.

To load a new detector engine onto an IDP-capable device:

1. From the menu bar, select Devices > IDP Detector Engine > Load IDP Detector Engine.
2. Click Next, then select the devices on which you want to load the detector engine.
3. Click Finish.

To download the DI attack object database update to your DI-capable devices:

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

Adding Objects (Optional)

Create address objects for the network components you want to protect with IDP. These components can be routers, servers, workstations, subnetworks, or any other object connected to your network. You can also create address object groups, which represent multiple address objects. (If you have previously created network objects for use with your FW/VPN security devices, you do not need to create them again.)

For more information about creating address objects, see “Configuring Address Objects” on page 227.

For more information about adding address object for standalone IDP sensors, see “IDP Concepts & Examples Guide.”

Configuring a Security Policy for IDP

Because the security module on the device processes traffic after the FW/VPN management module, you must configure a firewall rule to pass permitted traffic to the IDP rulebases. Enabling IDP functionality in a Security Policy is a two-step process: first enable a firewall rule to pass permitted traffic to the IDP rulebases, then create the IDP rules that detect and prevent malicious traffic from entering your network.
When creating a new Security Policy for your IDP deployment, we highly recommend you use a Security Policy template. Each Security Policy template contains the IDP rulebase and IDP rules that use the default actions associated with the Attack Object severity and protocol groups. You can customize these rules to work on your network as needed, such as selecting your own Address Objects as the Destination IP and choosing IDP actions and notifications that reflect your security needs.

If you do not use a Security Policy template, you must add the IDP rulebase manually, as detailed in “Adding the IDP Rulebases” on page 40.

**Configure Firewall Rules (ISG Only)**

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

When configuring the firewall rule, consider the following:

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

---

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

When operating the security device in transparent mode for and using as a dedicated IDP system, you do not need to configure additional firewall settings.

---

- For firewall rules that pass traffic to the IDP rulebases, the Install On column must include IDP-capable devices only.

**Setting the IDP Mode (ISG Only)**

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

To set the IDP mode:

1. In the main navigation tree, select **Security Policies**, then double-click the policy name in the **Security Policies** window to open the firewall rulebase.

2. In the **Rule Options** column of a firewall rule, select **IDP**.

3. Select one of the following modes:
Configuring IDP-Capable Devices Overview

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

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

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

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

### Adding the IDP Rulebases

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

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

  For a quick overview of creating rules in the IDP rulebase, see the following section (page 38); for complete details, see “Configuring IDP Rules” on page 350.

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

  Add the Exempt rulebase:

  - When an IDP rule uses attack object groups containing one or more attack objects that produce false positives or irrelevant log records.

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

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

  For details on creating rules in the Exempt Rulebase, see “Configuring Exempt Rules” on page 364.
The Backdoor Detection Rulebase—This rulebase detects backdoor traffic from components on your internal network. A “backdoor” is a mechanism installed on a host computer that facilitates unauthorized access to the system. Attackers who have already compromised a system often install a backdoor to make future attacks easier. However, when attackers enter commands to control a backdoor, they generate interactive traffic that your security device can detect.

Add this rulebase to your Security Policy when you want to configure rules that detect backdoor activity on your internal network. For details on configuring rules in the Backdoor Detection Rulebase, see “Configuring Backdoor Rules” on page 367.

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

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

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

1. In the main navigation tree, select Security Policies, then double-click the policy name in the Security Policies window.
2. Click the Add icon in the upper right corner of the Security Policy window and select Add > IDP, Exempt, or Backdoor Detection > Rulebase to open the selected rulebase tab.

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

To add a rule to a rulebase:

1. Click the rulebase tab for the rulebase in which you want to add a rule.
2. On the left side of the Security Policy window, click the Add icon to open a default rule.

For rules in the IDP rulebase, you define the type of network traffic to monitor, the attacks to detect, the action to be taken against matching traffic, and the notification you want to receive. Specifically, you must configure the following:

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

You configure the match criteria in the following IDP rulebase columns:
From Zone
Source
To Zone
Destination
Service

For details on configuring match criteria within the IDP rulebase, see “Defining Match For IDP Rules” on page 351.

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

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

- For details on selecting attacks within IDP rules, see “Configuring Attack Objects in IDP Rules” on page 357
- For details on IDP attack objects, see “Working with IDP Attack Objects” on page 237.
- For details on creating your own custom IDP attack objects, see “Configuring Custom DI/IDP Attacks” on page 240.

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

You configure IDP actions in the Action column of an IDP rule. For details, see “Defining Actions For IDP Rules” on page 356.

You configure IP actions in the IP Action column of an IDP rule. For details, see “Configuring IP Actions in IDP Rules” on page 359. (The IP Action column appears only when viewing the Security Policy in Expanded Mode. To change the view mode of a policy, from the menu bar, select View > Expanded Mode or Compact Mode).

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

You configure Notification settings in the Notification column of an IDP rule. For details, see “Configuring Notification in IDP Rules” on page 360.
Assign, Validate, and Install the Security Policy

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

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

2. Validate the security policy (optional).
   
   Validating a Security Policy can identify potential problems before you install it.
   1. Go to the menu bar.
   2. Click Devices > Policy > Validate Policy to open a Job Manager window, displaying job information and progress.
   
   If NetScreen-Security Manager identifies any problems in the policy during policy validation, it displays information about the problem at the bottom of the selected rulebase. For example, if you included a non-IDP capable security device in the Install On column of an IDP rule, policy validation displays a error message.

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

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

To view IDP log entries:

1. Go to the main navigation tree.
2. Select Log Viewer > DI/IDP Logs. The Log Viewer displays all IDP logs generated by the security device.

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

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

Maintaining IDP

Attackers are constantly devising new and better ways to infiltrate your network. Juniper Networks is busy too, discovering these new attacks and creating new attack objects to detect them—so you can prevent the attacks from entering your network. To ensure that the IDP security module and that your Security Policy remains highly effective against all emerging and evolving threats, we highly recommend that you perform frequent updates to the attack object database and to the IDP detection engine, detailed in Managing the Attack Database on page 197.

Creating IDP-Only Administrators

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

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

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

- Attack Update
- Create/View/Edit/Delete Policies
Simplifying Management

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

These features include:

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

Using Device Groups

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

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

Using Device Templates

A template is a predefined device configuration that helps you re-use common information. A domain can contain multiple templates, and you can use templates to quickly configure and deploy multiple devices. A device template looks much like a device configuration—the template page displays boxes for interfaces, zones, and virtual routers in which you can enter values. When you add a new device that uses similar information as a previously added device, you can use a device template to fill in specific configuration values so you do not have to re-enter information.
For example, you might create a generic NetScreen-5GT device template that you can use each time you add a device of that type. Or, you can apply multiple templates to the same device. You can map a maximum of 63 templates to the same device; you set the priority of the template to determine the order in which they applied.

For example, you might create the following templates:

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

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

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

### Merging Policies

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

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

### Using a Naming Convention

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

If your network is small, you might choose a simple naming convention, such as planet names, car models, or mountain names. When using this type of informal method to name your network components, be sure to choose a theme that is easily understood by both your users and administrators, and that still has room to grow. For example, you might use the naming convention. `<city>_<name>`, with a naming theme of Greek mythology figures; some sample device names might be `la_ns5gt_Athena`, `sf_ns5XT_Zeus`, or `oak_ns204_Hermes`.

If your network is larger, however, you need a more formal naming schema that is more descriptive of the network component’s location and purpose. Having a logical and standardized naming convention can help you quickly identify the appropriate administrator for the component, as well as quickly identify the component location of without having to review subnet tables.
A typical naming convention for large, distributed networks consists of a standardized location identification code, followed by the department code, a description of function, and a numerical sequence.

EXAMPLE: USING A NAMING CONVENTION FOR SECURITY DEVICES
You use the naming convention: nation_state_platform_name for your security devices. Your devices use names similar to the following:

- us_ca_ns5gt_01
- us_co_ns204_05
- us_tx_ns5200_10

EXAMPLE: USING A NAMING CONVENTION FOR ADDRESS OBJECTS
For address objects that represent networks or hosts, you use the following naming convention: state_function_service_00:

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

For example, the first Apache Web server installed in the state of California is: ca_ws_apache_01.

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

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

For example, Wendy Parker, working in Texas on a Windows 2000 Pro laptop, would see her machine name as: tx_wparker_m_2kpro.

Creating an Information Banner

Central Manager admins and regional server “super” admins have the ability to display an informational banner when users log into NSM. This banner is created using custom text that is stored on the server. Once it has been created, the banner is displayed a splash screen after users enter their login credentials. This text is used server-wide (which does not depend on user, role, domain, and so on). Users are unable to proceed into the NSM UI until they accept the message to continue. If this banner is used, users are required to accept the message each time they log in.

You can add an information banner from Central Manager or from a regional server.

Adding an Information Banner

This procedure assumes that a Central Manager admin is logged onto a Central Manager client or a super user is logged into a regional server.

To add an informational banner:

1. In the main navigation tree, select Server Manager > Servers.
2. Select the GUI server to which you want to add the banner server-wide.

Figure 10: Select the GUI Server in Central Manager
3. Enter the customized text in the **Log In Warning Message** text box, then click **OK**.

Figure 11: Setting Up an Information Banner

The message is immediately available to NSM users server-wide.

Figure 12: Information Banner Login Into Central Manager
4. Click Yes to access the GUI server.

You see the following message if you click No.

Figure 13: Access Denied to GUI Server

5. Click OK to return to the Login screen.

Modifying an Information Banner

This procedure assumes that a Central Manager admin is logged onto a Central Manager client or a super user is logged into a regional server and an information banner has been created.

To modify an informational banner:

1. In the main navigation tree, select Server Manager > Servers.

2. Double-click the GUI server to which you want to add the banner server-wide.

3. Change the customized text in the Log In Warning Message text box, then click OK.

The message is immediately available to all NSM users server-wide.

Deleting an Information Banner

This procedure assumes that a Central Manager admin is logged onto a Central Manager client or a super user is logged into a regional server and an information banner has been created.

To delete an informational banner:

1. In the main navigation tree, select Server Manager > Servers.

2. Double-click the GUI server to which you want to add the banner server-wide.

3. Enter the customized text in the Log In Warning Message text box, then click OK.

The message is immediately removed from the login screen to all NSM users server-wide.
Chapter 3
Configuring Role-Based Administration

This chapter details how to use the Juniper Networks NetScreen-Security Manager 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 (RBA), you can recreate this same permission structure in NetScreen-Security Manager.

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

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

This chapter contains the following sections:

- Role-Based Administration on page 52
- Using Role-Based Administration Effectively on page 53
- Configuring Role-Based Administration on page 57
Role-Based Administration

The NetScreen-Security Manager role-based administration (RBA) feature enables you to define strategic roles for your administrators, delegate management tasks, and enhance existing permission structures using task-based functions.

Use NetScreen-Security Manager to create a secure environment that reflects your current administrator roles and responsibilities. By specifying the exact tasks your NetScreen-Security Manager administrators can perform within a domain, you minimize the probability of errors and security violations, and enable a clear audit trail for every management event.

Domains

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

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

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

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

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

Domain selection is important 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. NetScreen-Security Manager uses a powerful, role-based access control system that enables you to create custom roles for individual administrators. Use role-based management to control administrative access to NetScreen-Security Manager functionality.
All NetScreen-Security Manager users are some type of admin. During NetScreen-Security Manager installation, you are prompted for a password for the (default) admin account for NetScreen-Security Manager; this admin account is the first administrator, and is therefore the super administrator. The super admin automatically has all permissions, and can create other domains, admins, and roles. As super admin, you specify who has what permissions for NetScreen-Security Manager functionality for the entire NetScreen-Security Manager system, a single domain, or specific functionality within a domain.

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

There are active and read-only System Administrators. All System Administrators, including those assigned a Read-Only role, can create and run their own reports.

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

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

NOTE: You cannot define a custom activity.

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

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

Using Role-Based Administration Effectively

The structure of your NetScreen-Security Manager domains should reflect both your existing network structure and your desired permission structure.

- **Network Structure**—Use multiple domains to segregate large, geographically distant networks into locally-managed sections.
- **Permission Structure**—Use multiple domains to segregate critical devices and systems from less important network areas, then restrict administrator access to devices in the critical domain.

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

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

**Enterprise Organizations**

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

**Geographical Divisions**

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

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

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

**NOC and SOC**

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

- NOC administrators focus on network connectivity and status.

- SOC administrators focus on network attacks and events associated with Security Policies.
Chapter 3: Configuring Role-Based Administration

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

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

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

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

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

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

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

### Service Providers

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

### Internal Network

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

### Managed Security Service Provider (MSSP)

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

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

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

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

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

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

Configuring Role-Based Administration

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

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

- **Administrators**—Configure administrators for NetScreen-Security Manager or IDP.
- **Roles**—View or edit default roles, or create your own custom roles for your NetScreen-Security Manager or IDP administrators.
- **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 RBA settings.

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

Creating Administrators

The super administrator (superadmin) automatically has full permissions for all subdomains, so you do not need to assign new subdomains to the superadmin. However, to assign a subdomain to another administrator, you must first create the administrator and specify their permissions within a selected subdomain.

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

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

Configuring General Settings

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

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

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

Configuring Authorization

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

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

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

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

NOTE: The superadmin has full permissions. You cannot change or delete permissions for the superadmin; you can only change the password. Because the superadmin has complete control over NetScreen-Security Manager functionality, we recommend that you consider the security of the superadmin password appropriately. If you forget or lose the superadmin password, please contact the Juniper Technical Assistance Center (JTAC).

RADIUS Authentication and Authorization

NetScreen Security Manager supports both local and RADIUS user authentication. It manages access control both through the local database and through the RADIUS server.

You are not required to define RADIUS users in the local NetScreen Security Manager database. The AUTH Handler looks at the local database to find the user then, if no match is found, to the RADIUS server. You can also define the role assignment for each user directly from the RADIUS server.

NOTE: You must configure your RADIUS server individually for each domain.

NetScreen Security Manager also supports a secondary RADIUS servers for admin authentication and authorization when the primary RADIUS server cannot be contacted.

There are two kinds of users: local users and RADIUS users. The local user is created locally and authentication data is stored in the local database. The default authentication mode is local mode. The RADIUS user is created only on a RADIUS server and can only be authenticated using a remote RADIUS server.

There are also two kinds of authentication modes for NetScreen Security Manager users: local mode and RADIUS mode. Both User and Domain can define these modes and Domain’s authentication mode is applied to all the users within it. User’s Authentication mode has a higher priority and can override Domain’s mode.

The NetScreen Security Manager user is authenticated based on the rules listed in Table 6.

Table 6: How to Authenticate Users

<table>
<thead>
<tr>
<th>Rule</th>
<th>User in Local Database</th>
<th>User Auth Mode</th>
<th>Domain Auth Mode</th>
<th>Authentication Results</th>
<th>Authorization</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Defined</td>
<td>Local</td>
<td>Local</td>
<td>Authenticates user locally.</td>
<td>Local</td>
</tr>
<tr>
<td>2</td>
<td>Defined</td>
<td>Local</td>
<td>Remote</td>
<td>Authenticates user locally first. If fails, RADIUS authentication is used.</td>
<td>Local</td>
</tr>
<tr>
<td>3</td>
<td>Defined</td>
<td>Remote</td>
<td>Local</td>
<td>Authenticates user remotely.</td>
<td>Local</td>
</tr>
<tr>
<td>4</td>
<td>Defined</td>
<td>Remote</td>
<td>Remote</td>
<td>Authenticates user remotely.</td>
<td>Local</td>
</tr>
</tbody>
</table>
Dictionary File

To authenticate local or remote users from a RADIUS server, you must first define role mapping assignments and domain names in NetScreen-Security Manager. If you use Steel Belted RADIUS, you can copy the NetScreen-Security Manager RADIUS dictionary to your RADIUS server.

This file (netscreen.dct) is available in the NetScreen-Security Manager. If you installed NetScreen-Security Manager using the default options, you can find the dictionary in the following location:

/usr/netscreen/GuiSvr/utils/netscreen.dct

RADIUS VSA Definition

RADIUS Vendor Specific Attribute is available to allow vendors to support their own extended attributes. If you use a RADIUS server other than Steel Belted RADIUS, you must enter the following NetScreen-Security Manager attributes in your RADIUS dictionary file.

These attributes are case sensitive and must be entered exactly as they appear below:

ATTRIBUTE NS-NSM-User-Domain-Name 26 [vid=3224 type1=220 len1=+2 data=string]
ATTRIBUTE NS-NSM-User-Role-Mapping 26 [vid=3224 type1=221 len1=+2 data=string]

When a user is defined only in RADIUS, you must define NS-NSM-User-Domain-Name and role mapping assignment. Auth Handler checks if the domain name matches the user’s login domain name when NetScreen-Security Manager authenticates the user. Role Mapping lists are used for NetScreen-Security Manager Access Control purposes.

Custom Roles

Figure 14, shows the format for a custom role. The format for the custom role of NS-NSM-User-Role-Mapping is shown below.

domainName1:domainName2.roleName

where:

- domainName1 is the domain that the current user can access
- domainName2 is the domain that the current role (roleName) belongs to

If you create a custom domain, NS-NSM-User-Domain-Name should include the domain’s full path. Do not omit the word “global” and you must include the full path for domainName. e.g. global.d1, global, or global.d2. (See Figure 14.)

Table 6: How to Authenticate Users

<table>
<thead>
<tr>
<th>Rule</th>
<th>User in Local Database</th>
<th>User Auth Mode</th>
<th>Domain Auth Mode</th>
<th>Authentication Results</th>
<th>Authorization</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Not Defined</td>
<td>—</td>
<td>Local</td>
<td>Authenticates user remotely.</td>
<td>Remote</td>
</tr>
<tr>
<td>6</td>
<td>Not Defined</td>
<td>—</td>
<td>Remote</td>
<td>Authenticates user remotely.</td>
<td>Remote</td>
</tr>
</tbody>
</table>
Figure 14: Creating Custom Domain

In Figure 14, users belong to domain d1 and role r1 is defined in domain1. Therefore, the domain name is global.d1 and the role is global.d1:global.d1.r1.

Pre-Defined Roles
The current predefined role names, which users can use, are listed below:

- Domain Administrator
- IDP Administrator
- Read-Only Domain Administrator
- Read-Only IDP Administrator
- Read-Only System Administrator
- System Administrator

Predefined roles do not belong to any domain. The format for predefined roles is:

DomainName1:(predefined role name)

where:

- DomainName1 is the domain that the current user can access
- predefined role name one of the options listed in the "Pre-Defined Roles" section above.

Example: If a user is in domain d1 with a role of IDP Administrator, the domain name is global.d1 and the role is global.d1:IDP Administrator.
Creating Roles

If a user is defined in the local database or defined in RADIUS server, NetScreen-Security Manager uses a role mapping list from the local database. The custom roles must be created in NetScreen-Security Manager. If the custom roles belong to a sub-domain, it must be created in that sub-domain. If the role is created in global domain, it is automatically inherited into the sub-domain and can be assigned to a sub-domain user.

NOTE: A role defined in sub-domain only belongs to that sub-domain.

Assigning Roles

If a user is defined in the local database, NetScreen-Security Manager uses a role mapping list from the local database. Otherwise, the RADIUS administrator must configure the role mapping list for each user on the RADIUS server.

Figure 15 through Figure 21 show examples of assigning predefined and custom roles through RADIUS. All examples assume that the user will be authenticated and authorized using RADIUS server.

Figure 15: User in domain “global” with a pre-defined role

![Figure 15: User in domain “global” with a pre-defined role](image)

Figure 16: User in domain “global” with custom role “r1”

![Figure 16: User in domain “global” with custom role “r1”](image)

The “r1” role was created in the NetScreen-Security Manager in “global” domain.
Figure 17: User in subdomain “d1” with a pre-defined role

Create the custom role “r1” in the sub-domain “d1.”

Figure 18: User in sub-domain “d1” with a custom role “r1”

Figure 19: Assigning multiple roles to a user in global domain

Roles “r1” and “r2” are the custom roles assigned to the user.
Figure 20: Assigning multiple roles to a user in sub-domain

Both “r1” and “r2” are the custom roles assigned to the user.

Figure 21: Assigning roles defined in domain “global”

The user role “r1” is defined in global domain, but the user has access to only a sub-domain d1 and therefore gets a the global role “r1.”

Figure 22: Assigning roles defined in domain “global” to sub-domain only

The user is defined in domain “global” but has access to sub-domains only. The user is a “Domain Administrator” in subdomain “d1,” but has a custom role r1 for subdomain “d2.”
Configuring Permissions

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

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

- **Domain Administrator**—Can perform all activities in the domain.
- **Read-Only Domain Administrator**—Can perform all read-only activities in the domain.
- **IDP Administrator**—Can perform all IDP activities. All firewall-specific activities are excluded.
- **Read-Only IDP Administrator**—Can perform all read-only IDP activities.
- **System Administrator**—Can perform all system-wide activities, Domain Administrator activities, and IDP Administrator activities.
- **Read-Only System Administrator**—Can perform all read-only system-wide activities and Domain Administrator activities.

As each default role contains activities that relate to the traditional responsibilities for a specific job title. Use a default role to quickly create NetScreen-Security Manager administrator or to create administrators 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 65.

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

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

Creating Roles

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

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

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

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

Table 7: Predefined NetScreen-Security Manager Administrator Activities

<table>
<thead>
<tr>
<th>Function</th>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action Attributes</td>
<td>View, Modify</td>
<td>The Action Manager is a node on the main navigation tree that enables you to configure the management system to forward logs generated within a specific domain or subdomain.</td>
</tr>
<tr>
<td>Admin Roles</td>
<td>View, Create, Edit, Delete</td>
<td>An admin role defines the access privileges for a NetScreen-Security Manager administrator.</td>
</tr>
<tr>
<td>Admins</td>
<td>View, Create, Edit, Delete</td>
<td>An admin is a user of the NetScreen-Security Manager management system.</td>
</tr>
<tr>
<td>Attack Update</td>
<td>N/A</td>
<td>This activity enables an admin to update the attack object database on the NetScreen-Security Manager system and on each managed device that supports Deep Inspection.</td>
</tr>
<tr>
<td>Audit Logs</td>
<td>View</td>
<td>An audit log records an administrative change (such as login, update, or policy change) to the managed devices or management system.</td>
</tr>
<tr>
<td>Backdoor Rulebase</td>
<td>Create, Edit, View</td>
<td>This activity enables an admin to manage the Backdoor Rulebase within a Security Policy. Rules configured in this rulebase are supported only on IDP capable security devices, such as the ISG 2000 or ISG 1000 running 5.0IDP1.</td>
</tr>
<tr>
<td>CLI-based Reports</td>
<td>N/A</td>
<td>This activity enables an admin to generate predefined and shared historical log reports using the guiSvrCli command utility.</td>
</tr>
<tr>
<td>CLI-based Security Update</td>
<td>N/A</td>
<td>This activity enables an admin to update the attack object database on the NetScreen-Security Manager system using guiSvrCli command utility.</td>
</tr>
<tr>
<td>Device Certificates</td>
<td>Generate and Upload, Get, Delete</td>
<td>A device certificate authenticates packets passing through a device.</td>
</tr>
</tbody>
</table>
### Function | Task | Description
--- | --- | ---
Device Configuration | View/Update | A device configuration is the modeled configuration that exists for a managed device within NetScreen-Security Manager.
Device Delta Config | View | (ScreenOS devices only) A device delta config is a report that details the differences between the device configuration running on the physical device and the modeled device configuration in NetScreen-Security Manager.
Device Firmware | Update | The device firmware is the ScreenOS software image used on the managed device.
Device Log Comments | Update | A device log comment is a user-defined description of a security event that is recorded in a device log.
Device Log Flags | Update | A device log flag is visual icon that can be assigned to a device log. Admins can assign flags to indicate severity, status, and other options to a device log.
Device Logs | View Hide and Unhide Purge | A device log records a security event that occurred on a security device.
Device Passwords | View | This activity enables an admin to view device passwords in configuration summaries and Job Manager information details. Note: All passwords handled by NetScreen-Security Manager are case-sensitive.
Device Reboot | Reboot | A device reboot is a reboot command sent to a managed device to power down, then power up.
Device Running Config | View | A device running config is a report that details the device configuration running on the physical device.
Device Software Keys | Install | A device software key provides enhances or adds functionality for a managed device.
Device Status Monitor | View | The device status monitor tracks the status security devices, VPN tunnels, and NSRP.
Device Web Category | Update | The device Web category list contains predefined Web categories used in Web filtering profiles. You can update the device Web category list from the system Web category list.
Devices, Device Groups, and Templates | View Create Edit Delete | ■ A device is a security 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.
Firewall Rulebases | Create/Edit View | The firewall rulebases (Zone and Global) in a Security Policy contain rules that handle traffic passing through the firewall. These activities enable an admin to control and/or view rules in the firewall rulebases.
HA for guiSvrClusterMgr | N/A |  
Historical Log Reports | View | An historical log report is a report generated using historical log entries. If an admin can view historical log reports, then that admin can also view shared historical log reports and their definitions.
IDP Profiler Operations | View Purge Profiler Data | This activity enables an admin to view the Profiler. It also enables an admin to purge data in the ProfilerDB.
<table>
<thead>
<tr>
<th>Function</th>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDP Rulebase</td>
<td>Create</td>
<td>This activity enables an admin to manage the IDP Rulebase within a Security Policy. Rules configured in this rulebase are supported only on IDP capable security devices, such as the ISG 2000 or ISG 1000 running 5.0IDP1.</td>
</tr>
<tr>
<td></td>
<td>Edit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>View</td>
<td></td>
</tr>
<tr>
<td>Infranet Controller Operations</td>
<td>N/A</td>
<td>This activity enables an admin to configure a device to interoperate with an Infranet Controller.</td>
</tr>
<tr>
<td>Investigative Log Reports</td>
<td>View</td>
<td>The Log Investigator generates investigative log reports based on selected criteria. This activity enables an admin to view those log reports.</td>
</tr>
<tr>
<td>Job Status Logs</td>
<td>Purge</td>
<td>Each time NetScreen-Security Manager performs a task for which a job is created, Job Manager creates a job status log. This activity enables an admin to purge those logs from the management system.</td>
</tr>
<tr>
<td>Jobs</td>
<td>View</td>
<td>A job is a task that NetScreen-Security Manager performs, such as updating a device, generating a device certificate request, and importing a device.</td>
</tr>
<tr>
<td>Multicast Rulebases</td>
<td>Create/Edit</td>
<td>The multicast rulebase in a Security Policy contains multicast rules, which can handle IGMP and PIM-SM traffic. These activities enable an admin to control and/or view rules in the multicast rulebase.</td>
</tr>
<tr>
<td></td>
<td>View</td>
<td></td>
</tr>
<tr>
<td>NSRP Monitor</td>
<td>View</td>
<td>NSRP Monitor tracks NSRP statistics. To enable NetScreen-Security Manager to track these statistics, you must enable “NSRP Monitor” in the NSRP properties for each cluster device.</td>
</tr>
<tr>
<td>Security Policies</td>
<td>View</td>
<td>A policy is a set of rules that determines how a device handles traffic passing through the firewall.</td>
</tr>
<tr>
<td></td>
<td>Create</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Edit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Delete</td>
<td></td>
</tr>
<tr>
<td>Policy Lookup Table</td>
<td>Modify</td>
<td>A rulebase in a Security Policy contains rules that manage specific types of traffic passing through the managed device. These activities enable an admin to delete a rulebase.</td>
</tr>
<tr>
<td>Rulebases</td>
<td>Delete</td>
<td>A rulebase in a Security Policy contains rules that manage specific types of traffic passing through the managed device. These activities enable an admin to delete a rulebase.</td>
</tr>
<tr>
<td>Servers</td>
<td>View</td>
<td>The Device Server and GUI Server comprise the NetScreen-Security Manager System.</td>
</tr>
<tr>
<td></td>
<td>Create</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Edit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Delete</td>
<td></td>
</tr>
<tr>
<td>Shared Historical Log Report</td>
<td>View</td>
<td>A shared historical log report is a user-defined historical log report that is available to users with the appropriate permissions in a domain. These reports appear under “Shared Reports” in the UI and can be generated offline with the guiSvrCli utility. If an admin can create shared historical log reports, then that admin can also move a report from “My Reports” to “Shared Reports”. An admin requires permission to delete shared historical log reports in order to move a report from “Shared Reports” to “My Reports”.</td>
</tr>
<tr>
<td></td>
<td>Create</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Edit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Delete</td>
<td></td>
</tr>
<tr>
<td>Shared Objects and Groups</td>
<td>View</td>
<td>An object contains re-usable information. Shared objects include address book objects, schedule objects, attack objects, service objects, and user objects.</td>
</tr>
<tr>
<td></td>
<td>Create</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Edit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Delete</td>
<td></td>
</tr>
</tbody>
</table>
### Subdomains and Groups

<table>
<thead>
<tr>
<th>Function</th>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subdomains and Groups</td>
<td>View</td>
<td>A subdomain is a separate, unique representation of other networks that</td>
</tr>
<tr>
<td></td>
<td>Create</td>
<td>exist within your larger network.</td>
</tr>
<tr>
<td></td>
<td>Edit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Delete</td>
<td></td>
</tr>
</tbody>
</table>

### Supplemental CLIs in Devices & Templates

<table>
<thead>
<tr>
<th>Function</th>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supplemental CLIs</td>
<td>Edit</td>
<td>The Supplemental CLI option enables you to configure features on security</td>
</tr>
<tr>
<td>in Devices &amp; Templates</td>
<td></td>
<td>devices not yet formally supported in NetScreen-Security Manager. This</td>
</tr>
<tr>
<td></td>
<td></td>
<td>applies to security devices running a future release of ScreenOS.</td>
</tr>
</tbody>
</table>

### System Status Monitor

<table>
<thead>
<tr>
<th>Function</th>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Status Monitor</td>
<td>View</td>
<td>The system status monitor displays the status of NetScreen-Security Manager</td>
</tr>
<tr>
<td></td>
<td></td>
<td>servers (GUI Server and Device Server) and the processes running on each</td>
</tr>
<tr>
<td></td>
<td></td>
<td>server.</td>
</tr>
</tbody>
</table>

### System Web Category

<table>
<thead>
<tr>
<th>Function</th>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Web Category</td>
<td>Update</td>
<td>The system Web category list contains predefined Web categories used in Web</td>
</tr>
<tr>
<td></td>
<td></td>
<td>filtering profiles. You can update the system Web category list from the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>master Web category list maintained by SurfControl.</td>
</tr>
</tbody>
</table>

### Troubleshoot Devices

<table>
<thead>
<tr>
<th>Function</th>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Troubleshoot Devices</td>
<td></td>
<td>The Troubleshoot option in the Device Monitor enables you to query the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>status of a security device.</td>
</tr>
</tbody>
</table>

### VPN Monitor

<table>
<thead>
<tr>
<th>Function</th>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN Monitor</td>
<td>View</td>
<td>VPN Monitor tracks VPN tunnel statistics. To enable NetScreen-Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Manager to track these statistics, you must enable “VPN Monitor” in the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Gateway properties for each VPN.</td>
</tr>
</tbody>
</table>

### VPNs

<table>
<thead>
<tr>
<th>Function</th>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPNS</td>
<td>View</td>
<td>A VPN is a virtual private network that exists between two or more security</td>
</tr>
<tr>
<td></td>
<td>Create</td>
<td>devices, extranet devices, or RAS users.</td>
</tr>
<tr>
<td></td>
<td>Edit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Delete</td>
<td></td>
</tr>
</tbody>
</table>

Some activities might not be listed in the preceding table, but are listed in NetScreen-Security Manager.

### IDP Administrator Role

The superadmin creates IDP Administrator and IDP Read-Only Administrator roles. These roles include IDP-specific activities and excluded firewall-specific activities. For example, shared objects used for firewall/VPN configuration such as Web Filtering Certificate Authorities are not included.

As of Release 2006.1, the Create Devices, Device Groups, & Templates role does not allow permission to run the following directives:

- Import Admin
- Export Device Config To File
- Import Device Config To File

The role Import Device Admins allows permission to run the Import Admin directive.

A new role (Export/Import DM to File) is created to allow permission to run the Export Device Config To File and Import Device Config From File directives.
Roles and Permissions

As of Release 2005.3, the “Edit Devices, Device Groups, & Templates” role no longer allows permission to run the directive(s) listed in Table 8. The following new activities(s) provide permission for the same directive(s) as listed in the table.

Table 8: Changes to “Edit Devices, Device Groups, & Templates” Role

<table>
<thead>
<tr>
<th>Activity</th>
<th>Directive(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Configlet</td>
<td>View Configlet</td>
</tr>
<tr>
<td>Edit Device Admin</td>
<td>Set Root Admin (4.x device only)</td>
</tr>
<tr>
<td></td>
<td>Set Admin Ports (4.x device only)</td>
</tr>
<tr>
<td></td>
<td>Set Admin SSH Enable/ Disable (4.x device only)</td>
</tr>
<tr>
<td>Failover Device</td>
<td>Failover</td>
</tr>
<tr>
<td>Device BGP Operations</td>
<td>Modify BGPPeer Session</td>
</tr>
<tr>
<td></td>
<td>BGP Refresh Route</td>
</tr>
<tr>
<td></td>
<td>BGP Update Route on Peer</td>
</tr>
<tr>
<td>Update AV Pattern</td>
<td>Update AV Pattern</td>
</tr>
<tr>
<td>Get Entitlement from Entitlement Server</td>
<td>Get Entitlement from Entitlement Server</td>
</tr>
<tr>
<td>Check Config Sync Status</td>
<td>Check Config Sync</td>
</tr>
<tr>
<td>Intranet Controller Operations</td>
<td>Connect To Intranet Controller</td>
</tr>
<tr>
<td></td>
<td>Disconnect From Intranet Controller</td>
</tr>
</tbody>
</table>

As of Release 2005.3, View Devices, Device Groups, & Templates role no longer allows permission to run the directive(s) listed in Table 9. The following new activities(s) provide permission for the same directive(s) as listed in the table.

Table 9: Changes to View Devices, Device Groups, & Templates Role

<table>
<thead>
<tr>
<th>Activity</th>
<th>Directive(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Site Survey</td>
<td>Site Survey</td>
</tr>
</tbody>
</table>

Assigning and Viewing Custom Roles

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

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

Viewing Logged In Administrators

NetScreen-Security Manager lets you view information associated with all the administrators currently logged into the system. This information includes the following columns:

- **Home Domain** — Indicates the name of the domain in which the administrator was created.
Chapter 3: Configuring Role-Based Administration

- **Admin Name** — Lists the name of the administrator who is logged in.

- **Status** — Indicates if a user is active or inactive (no activity for more than 5 minutes). Once the administrator’s status is inactive, NetScreen-Security Manager sends an update to the server at 1-minute intervals. This update automatically refreshes the screen with the new information. Once active, NetScreen-Security Manager sends another update to the server that the status has changed.

- **IP Address** — Lists the administrator’s IP address.

- **Locked Object** — Provides a detailed list about the objects locked by each administrator listed. These locked objects include object identifiers, length of time the object is locked, the lock type, and so on.

Using this information, system administrators can monitor and manage users more effectively.

Access to this feature is granted only to system administrators and read-only administrators. You can access this information from the Tools menu by selecting the Logged In Administrators menu item. By default, this activity is assigned to the predefined system-administrator role.

**Creating Subdomains**

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

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

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

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

**Viewing Current Domain Detail**

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

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

- To authenticate administrators when they log into the NetScreen-Security Manager system
- To authenticate RAS users in VPNs
For step-by-step instructions on configuring a RADIUS authentication server to authenticate administrators and users, see the NetScreen-Security Manager Online Help topic “Editing the Domain Contact.”

**Domain Versioning**

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

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

An archived domain version displays the modules (Device Manager, Security Policies, Log Investigator, and so on) that were saved during the versioning process. Because the versioning process saves only the modules that were changed, some modules might not appear. You cannot edit objects, policies, or other parameters for an archived domain version.

To return to the current domain version, click **Tools > Select Domain Version**, and select the most recent domain version.

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

**EXAMPLE: CONFIGURING ROLE-BASED ADMINISTRATION**

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

To configure this domain structure, use the following process:

- Create the subdomains
- Create the subdomain administrators
■ Create the read-only customer administrator

■ Login as each administrator (for verification)

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

1. Log in to the global domain as the superadmin.

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

3. Click the **Subdomains** tab, then click the Add icon to create a subdomain for the first customer. Configure the following four subdomains:
   - MA_company1
   - NH_company2
   - RI_company3
   - VT_company4

4. Click **OK** to save your changes.

**Step 2: Create the Subdomain Administrator**
In this step, you create a subdomain administrator with full permissions for the domain.

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

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

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

4. Click **OK** to save your changes.

5. Repeat for each subdomain.
Step 3: Create the Viewing and Reporting Administrator

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

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

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

3. In the **Roles** tab, click the Add icon. Name the new role, add an optional comment, choose a color, then select activities and reporting permissions for this domain.

4. Click **OK** to save your changes.

5. In the **Administrators** tab, click the Add icon to create the customer administrator for this domain:
   - In the **General Properties** tab, enter a name, color, and contact information for the admin.
   - In the **Authorization** tab, leave the default authentication as **Local** and configure a password for the admin.
   - In the **Permissions** tab, click the Add icon, then configure the role as Viewing & Reporting and the Domain as MA_company1.

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

   ![Manage Administrators and Domains: Administrators Tab](image)

7. Click **OK** to save your changes.

8. Repeat for each subdomain.
Step 4: Verify Administrator Accounts

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

- **Logging in as the Domain Administrator**—To log in as the domain administrator, in the login screen, enter the subdomain/domain admin name (MA_company1/MA_Admin), the password, and the GUI Server IP address.

  Click OK to log in. The NetScreen-Security Manager navigation tree and main display area appear. Because the domain admin account has full permissions for the domain, the UI displays all modules and enables all functionality for the domain. However, the domain menu (at the top of the navigation tree) displays only the current domain, restricting the domain admin to that domain.

  Repeat for each subdomain and domain admin.

- **Logging in as the Customer Administrator**—To log in as the customer admin, in the login screen, enter the subdomain/domain admin name (MA_company1/Customer_Admin), the password, and the GUI Server IP address.

  Click OK to log in. The NetScreen-Security Manager navigation tree and main display area appear. Because the customer admin account has permission only for viewing and reports, the UI displays only the modules that are used 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.
Part 2
Integrating

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

Part 2 contains the following chapters:

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

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

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

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

After you have integrated your security devices into the management system and are familiar with the device configuration, updating, and management features in the UI, you are ready to begin building the Security Policies and VPNs that control your network traffic, as detailed in Part 3, “Managing” on page 221.
Chapter 4
Adding Devices

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

Juniper Networks NetScreen-Security Manager can manage all Juniper Networks security devices running Juniper Networks ScreenOS 4.x and higher (except 4.0.2), and IDP 4.X and higher. NetScreen-Security Manager can also manage vsys configurations, NSRP clusters, Vsys clusters, and extranet devices.

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

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

NOTE: If you have been managing your IDP Sensors using the IDP Management Server and UI, you should migrate your Sensors instead of adding them manually. See the IDP-NetScreen-Security Manager Migration Guide for procedures and additional information.

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

This chapter contains the following sections:

- About Device Creation on page 80
- Before You Begin on page 82
- Importing Devices on page 92
- Modeling Devices on page 104
- Using Rapid Deployment (ScreenOS only) on page 113
- Adding Other Device Types on page 122
- Adding Many Devices (ScreenOS only) on page 131
About Device Creation

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

You can add the following types of devices:

- **Security devices**—A security device or system (such as a NetScreen-5GT device, an ISG device, or an IDP Sensor) is a device that manages firewall, VPN, and/or IDP activities on your network. The “Importing Devices” and “Modeling Devices” sections of this chapter detail how to add an existing or new security device into NetScreen-Security Manager. For details on adding many devices or systems at one time, see “Adding Many Devices (ScreenOS only)” on page 131.

  Adding an IDP Sensor to NetScreen-Security Manager does not migrate existing settings. If you have existing IDP Sensors that are managed by an IDP Management Server, you should migrate those Sensors using the instructions in the IDP-NetScreen Security Manager Migration Guide.

- **Vsys devices**—A vsys is a virtual device that exists within a physical security device. For details on adding vsys devices, see Adding Vsys Devices on page 122.

- **Clusters**—A cluster is two security devices joined together in a high availability configuration to ensure continued network uptime. For details on adding clusters, see “Adding a Cluster” on page 127.

- **Vsys clusters**—A Vsys cluster device is a vsys device that has a cluster as its root device. For details on adding Vsys clusters and Vsys devices, see “Adding a Vsys Cluster and Vsys Cluster Members” on page 128.

- **Extranet devices**—An extranet device is a third party device or device not managed by NSM. For details on adding extranet devices, see “Adding an Extranet Device” on page 126.

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

Determine Device Status

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

NOTE: To import device configurations, the connection between the NetScreen-Security Manager system and the managed device must be at least 28.8kbps. For details on installing NetScreen-Security Manager on your network, refer to the NetScreen-Security Manager 2004 FP3 Installer’s Guide.

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

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

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

**Verify Device Configuration**

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

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

**Managing the Device**

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

If you delete a device that was added using Rapid Deployment (described on page 113), you must also re-create the configlet and install it again on the device.

Before You Begin

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

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

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

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

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

Importing vs. Modeling

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

Importing Device Configurations

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

After you have imported several devices, you can start using system-level management features, such as the policy merge tool (merge several device Security Policies into a single, efficient policy that is easy to maintain), device groups (group devices by function, location, or platform to make updating easier), and the VPN Manager (create VPNs across multiple devices quickly).
If you modify a device and import or re-import the device into NSM, a new policy is automatically created using the following naming syntax: device_1. (Each new policy increments the name.) Devices are not assigned to the new policy. If you re-import a device with no changes then a duplicate policy is not created.

**Importing and Templates**

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

**Modeling Device Configurations**

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

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

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

**Device Add Process**

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

The amount of manual involvement when adding a device to NetScreen-Security Manager depends on several factors, such as if you are importing a deployed device, activating a modeled device, the software version the device is running, and the type of IP address (static or dynamic) the device uses to connect to the management system. The procedures below guide you through the process.
Selecting the Domain

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

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

- **Add device to the global domain**—Ensure that you are in the global domain and begin the device creation process.

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

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

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

Domain selection is critical when using VPNs. You can create VPNs only between devices within the same domain. If you need to add a device to a VPN in a different domain, add the device as an extranet device in the domain that contains the VPN, then add the extranet device to the VPN (as shown in Figure 24).

![Figure 24: Connecting Devices from Different Domains in VPNs](image)
Adding Single or Multiple Devices

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

When adding a single security device, you use the Add Device Wizard to create the device object in NetScreen-Security Manager. To activate a modeled device and/or create a configlet, you use the Activate Device Wizard. You can import or model device configurations from a device running ScreenOS 4.0.x or higher, or IDP 4.x or higher.

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

You can use the Add Many Devices wizard for the following tasks:

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

Additionally, you can use the Activate Many Devices wizard to create configlets for and activate multiple ScreenOS 5.x devices at one time for use with Rapid Deployment. However, you cannot activate multiple ScreenOS 5.x devices without creating configlets. For details, see “Adding Many Devices (ScreenOS only)” on page 131.

Determining ScreenOS Version (ScreenOS only)

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

- For devices that use a static IP address, you do not need to specify the ScreenOS version. NetScreen-Security Manager automatically detects this information during the add process.
- For undeployed devices or for devices that use a dynamically-assigned IP address, you must specify the ScreenOS version of the device. NetScreen-Security Manager validates the version during the model or add process.

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

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

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

- Trust-Untrust Port Mode
- Home-Work Port Mode
- Dual-Untrust Port Mode
- Combined Port Mode
- Trust-Untrust-DMZ Port Mode
- Trust/Untrust/DMZ (Extended) Mode
- DMZ-Dual-Untrust Port Mode

Trust-Untrust Port Mode

Trust-Untrust mode is the default port mode. See Figure 25 for port, interface, and zone bindings.

![Figure 25: Trust-Untrust Port Mode Bindings](image)

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

Home-Work mode binds interfaces to the Untrust security zone and to Home and Work security zones. The Home and Work zones enable you to segregate users and resources in each zone. In this mode, default policies permit traffic flow and connections from the Work zone to the Home zone, but do not permit traffic from the Home zone to the Work zone. By default, there are no restrictions for traffic from the Home zone to the Untrust zone. See Figure 26 for port, interface, and zone bindings.

Figure 26: Home-Work Port Mode Bindings

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

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

Dual-Untrust Port Mode

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

See Figure 27 for port, interface, and zone bindings.
Figure 27: Dual-Untrust Port Mode Bindings

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

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

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

### Combined Port Mode

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

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

See Figure 28 for port, interface, and zone bindings.

Figure 28: Combined Port Mode Bindings

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

- Binds the Untrusted Ethernet port to the ethernet4 interface, which is bound to the Untrust zone.
Before You Begin

Chapter 4: Adding Devices

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

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

Trust-Untrust-DMZ Port Mode

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

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

See Figure 29 for port, interface, and zone bindings.

Trust Zone

DMZ Zone

Untrust Zone

The ethernet3 interface is the primary interface to the Untrust zone. You can bind the serial interface as a backup interface to the Untrust zone.

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

Trust-Untrust/DMZ (Extended) Mode

Trust/Untrust/DMZ (Extended) mode binds interfaces to the Untrust, Trust, and DMZ security zones, allowing you to segregate web, email, or other application servers from the internal network. See Figure 30.
Before You Begin

Table 10 provides the Extended mode interface-to-zone bindings.

Table 10: Extended Bindings

<table>
<thead>
<tr>
<th>Port</th>
<th>Interface</th>
<th>Zone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Untrusted</td>
<td>Ethernet1</td>
<td>Trust</td>
</tr>
<tr>
<td>Untrusted</td>
<td>Ethernet1</td>
<td>Trust</td>
</tr>
<tr>
<td>3</td>
<td>Ethernet2</td>
<td>DMZ</td>
</tr>
<tr>
<td>4</td>
<td>Ethernet2</td>
<td>DMZ</td>
</tr>
<tr>
<td>Modem</td>
<td>Serial</td>
<td>Untrust</td>
</tr>
</tbody>
</table>

DMZ-Dual-Untrust Port Mode

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

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

See Figure 31 for port, interface, and zone bindings.

Figure 31: DMZ Dual Untrust Port Mode

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

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

To enable failover instead of passing traffic simultaneously, you can configure the failover settings in the device configuration after you have added the device to the management system. For details, see “NetScreen-Security Manager: Configuring Firewall/VPN Devices”.

Port Mode Summary

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

Table 11: Security Device Port Mode Summary (Part 1)

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

Table 12: Security Device Port Mode Summary (Part 2)

<table>
<thead>
<tr>
<th>Port</th>
<th>Combined Mode</th>
<th>Trust/ Untrust/ DMZ Mode</th>
<th>DMZ/ Dual Untrust Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Interface</td>
<td>Zone</td>
<td>Interface</td>
</tr>
<tr>
<td>Untrusted</td>
<td>ethernet4</td>
<td>Untrust</td>
<td>ethernet3</td>
</tr>
<tr>
<td>1</td>
<td>ethernet1</td>
<td>Work</td>
<td>ethernet1</td>
</tr>
<tr>
<td>2</td>
<td>ethernet2</td>
<td>Home</td>
<td>ethernet1</td>
</tr>
<tr>
<td>3</td>
<td>ethernet2</td>
<td>Home</td>
<td>ethernet2</td>
</tr>
<tr>
<td>4</td>
<td>ethernet3</td>
<td>Untrust</td>
<td>ethernet2</td>
</tr>
<tr>
<td>Modem</td>
<td>N/A</td>
<td>N/A</td>
<td>serial</td>
</tr>
</tbody>
</table>

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

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

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

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

Importing Devices

NetScreen-Security Manager can import device configurations from devices running ScreenOS 4.x or later, or IDP 4.x or later. The process differs slightly between ScreenOS 5.x devices, ScreenOS 4.0.x devices, and IDP devices.

When importing ScreenOS 4.0.x devices, the management system connects to the device and imports the CLI command statements that detail the device configuration. The connection is secured using a standard encryption method; multiple, temporary connections between the management system and device are possible.

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

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

For details on adding multiple devices at one time, see “Adding Many Devices (ScreenOS only)” on page 131.

Requirements

To import a single device:

- The physical device must have Telnet or SSH enabled.

---

**NOTE:** Importing the running configuration from a device completely overwrites all configuration information stored within NetScreen-Security Manager for that device. To help avoid accidental configuration overwriting, when you attempt to import a configuration from a currently managed security device, NetScreen-Security Manager prompts you for confirmation to import.

**NOTE:** IDP rulebases cannot be imported.
Chapter 4: Adding Devices

You must have the device connection information (IP address, connection method) and device admin name and password available. For stand-alone IDP Sensors, you must also have the root password.

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

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

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

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

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

Adding Devices with Static IP Addresses

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

ScreenOS 4.0.x Devices

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

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

2. In Device Manager, click the Add icon and select Device to open the Add Device wizard.

   - Enter a name and select a color to represent the device in the UI.
   - Select Device is Reachable (default).

3. Click Next to display the Specify Connection Settings dialog box. Enter the connection information:

   - Enter the IP Address of the security device.
   - Enter the username of the device admin.
Enter the password for the device admin.

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

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

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

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

4. The wizard displays the autodetected device information. Verify that the device type, ScreenOS version, and the device serial number are correct, then select the Device Server connection:

   ■ Use the default settings to configure the device to connect to the NetScreen-Security Manager Device Server IP address and port.

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

5. Click Next.

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

7. 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.

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

Click OK to add the NACN Arbitrator.

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

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

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

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

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

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

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

2. In Device Manager, click the Add icon and select Device to open the Add Device wizard.
   - Enter a name and select a color to represent the device in the UI.
   - Select Device is Reachable (default).

3. Click Next to open the Specify Connection Settings dialog box.

4. Enter the following connection information:
   - Enter the IP Address of the security device.
   - Enter the username of the device admin.
   - Enter the password for the device admin.

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

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

    If you selected Telnet, click Next and go directly to step 4.
If you selected an SSH version, click Next to open 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.

5. After the wizard displays the autodetected device information, verify that the device type, ScreenOS version, and the device serial number are correct.

6. Click Next to add the device to NSM.

7. After the device is added, click Next to import the device configuration.

8. Click Finish to complete the **Add Device** wizard.

9. Double-click the device in Device Manager to view the imported configuration.

---

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

---

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

**IDP 4.0 Sensors**

IDP Sensors running versions of the IDP software earlier than 4.0 cannot be imported. If those Sensors are already being managed by IDP Manager, migrate your IDP Management Server and the Sensors with it. Refer to the IDP-NetScreen-Security Manager Migration Guide for more information.

You need to upgrade unmanaged Sensors to 4.x before adding them to NetScreen-Security Manager. See the IDP Installer’s Guide for more information.

To import an IDP 4.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** to open the **Add Device** wizard.

   - 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.

4. Enter the following connection information:

   - Enter the IP Address of the Sensor.
   - Enter the username of the device admin.
- Enter the password for the device admin.
- Enter the password for the device root user.

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

- Select the connection method (SSH Version 2) and the port number for the selected service.
- Select the Port Number. The default (port 22) is recommended.

5. Click **Next** to open the **Verify Device Authenticity** dialog box. The device wizard displays the RSA Key Fingerprint information.

6. After you have verified the key, click **Next** to display the autodetect device information. This will take a moment.

7. Verify that the device type, OS version, device serial number, and device mode are correct.

8. Click **Next** to have NSM add the Sensor as a managed device.

9. Click **Next** to have NSM import settings already present on the Sensor.

10. Click **Finish** to update the Sensor with the Juniper Networks Recommended policy. (Only applies to IDP 4.1 or higher. IDP 4.0 Sensors cannot use the Recommended policy.)

The **Job Information** dialog appears showing the status of the Update Device job.

11. After the Update Device job 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** to open the **Add Device** wizard.
Enter a name and select a color to represent the device in the UI.

Select **Device is not Reachable**.

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

- Enter the device type and specify the ScreenOS version that is running on the device.
- If desired, enable **Transparent Mode**.
- Select the Device Server connection: Use the default settings to configure the device to connect to the NetScreen-Security Manager Device Server IP address and port. Use a MIP to configure the device to connect to the NetScreen-Security Manager Device Server through a mapped IP address and port.

4. Click **Next** to open the **Configure NACN and Global-PRO Logging** dialog box.

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

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

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

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

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

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

**NOTE:** The device admin can also use a console connection to execute the commands on the physical device. However, the commands must be entered three at a time to ensure that the device receives all commands.
Chapter 4: Adding Devices

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

6. Click **Finish** to complete the **Add Device** wizard, which adds the new device in the **Device Manager** list.

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

**ScreenOS 5.x Devices**

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

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

2. In Device Manager, click the Add icon and select **Device** to open the **Add Device** wizard.

   - Enter a name and select a color to represent the device in the UI.
   - Select **Device is not Reachable**.
   - Select the **Device Server connection**: Use the default settings to configure the device to connect to the NetScreen-Security Manager Device Server IP address and port. Use a MIP to configure the device to connect to the NetScreen-Security Manager Device Server through a mapped IP address and port.

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

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

5. Click **Next**.

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

---

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

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

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

7. **To check** the device configuration status, mouseover the device in Device Manager (you can also check configuration status in Device Monitor):

   - Before the device connects, the status displays **Waiting for 1st connect**, indicating that the management system is waiting for the device to connect. (This event occurs very quickly and might not display.)
   
   - After the device connects, the status displays **Import Needed**, indicating that the device has connected but the management system has not imported the device configuration yet.

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

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

---

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

---

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

**IDP 4.0 Sensors**

IDP Sensors running versions of the IDP software earlier than 4.0 cannot be imported. If those Sensors are already being managed by IDP Manager, migrate your IDP Management Server and the Sensors with it. See the IDP-NetScreen-Security Manager Migration Guide for more information.

You need to upgrade unmanaged Sensors to 4.x before adding them to NetScreen-Security Manager. See the IDP Installer’s Guide for more information.

**To import** an IDP 4.0 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** to open the **Add Device** wizard.

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

3. Click **Next**.
   - Enter the device type.
   - Specify the OS version that is running on the device.
   - Leave Support Level set on **Full Support**.

4. Click **Next**.
   - The wizard automatically enters the Unique External ID for the device. This ID number represents the device within the management system.
   - Click **Set Password** to specify the First Connection One Time (OTP) password 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,
   - Click **Finish** to complete the **Add Device** wizard to add the new device in the **Device Manager** list.

5. Log into the device as root and run the commands.

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 Imported Device Configurations**

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

**Using Device Monitor**

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

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

**Using Device Manager**

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

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

---

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

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

---
Using Job Manager

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

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

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

Using Configuration Summaries (ScreenOS only)

NetScreen-Security Manager provides three configuration summaries to help you manage device configurations and prevent accidental misconfiguration. You should use configuration summaries after you import a device to ensure that the management system imported the physical device configuration as you expected.

Configuration summaries help with ongoing device maintenance, too, particularly for devices on which a local device administrator has been troubleshooting using CLI commands or the WebUI. Because the UI device configuration can overwrite the physical device configuration, you should always confirm the commands that are sent to the device.

Config Summary

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

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

Delta Configuration Summary (ScreenOS only)

A delta configuration summary shows you the differences between the configuration you see in the NetScreen-Security Manager UI and the configuration on the physical device. To get a Delta Configuration Summary, from the menu bar, click Devices Configuration > Summarize Delta Config to display a list of security devices to which you have access. Select the device you just imported and click OK. NetScreen-Security Manager queries the physical device to obtain a list of all CLI commands used in the device configuration, compares that list with the UI device configuration, and generates a summary report of all differences, or deltas discovered.
For a just-imported device, the delta config summary should display minimal deltas, meaning that very few differences exist between the configuration on the physical device and the configuration in the UI. NetScreen-Security Manager automatically imports your VPNs and displays the VPN policies; however, NetScreen-Security Manager does not create VPN abstractions for your VPN policies.

**Get Running Config**

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

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

**Modeling Devices**

For undeployed devices, you can create a device configuration in NetScreen-Security Manager then install that device configuration on the physical device. For ScreenOS 5.x devices, you can use Rapid Deployment (RD) to quickly provision multiple devices in non-technical environments. See “Using Rapid Deployment (ScreenOS only)” on page 113 for details.

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

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

For details on modeling multiple devices at one time, see “Adding Many Devices (ScreenOS only)” on page 131.

**Requirements**

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

To activate a device:

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

---

*NOTE:* All passwords handled by NetScreen-Security Manager are case-sensitive.
The device must be staged (physically connected to your network and can access network resources).

The device must have at least one interface that has an IP address. Devices that use dynamically assigned IP address must also support NACN.

**Modeling a Device**

To add a device:

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

2. In Device Manager, click the Add icon and select Device. The device wizard appears.
   - Enter a name and select a color to represent the device in the UI.
   - Select Model Device.

3. Click Next to display the New Device platform dialog box. Enter the device platform and OS version.

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

5. (ScreenOS devices only) Enable transparent mode, if desired.

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

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

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

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

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

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

Activating a Device

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

Devices with Static IP Addresses

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

ScreenOS 4.0.x Devices

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

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

2. Right-click the device and select Activate Device to display the Activate Device wizard.

3. Select Device Deployed and IP is Reachable.

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

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

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

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

5. The wizard displays the autodetected device information. Verify that the device type, OS version, and the device serial number are correct, then select the Device Server connection:

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

6. Click Next.

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

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

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

---

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

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

---

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

The device cannot connect to NetScreen-Security Manager until these commands are executed on the physical device.
9. 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.

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

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

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

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

2. Right-click the device and select **Activate Device** to display the Activate Device wizard.

3. Select **Device Deployed and IP is Reachable**.

4. Click **Next** to display the Specify Connection Settings dialog box. Enter the connection information:
   - Enter the IP Address of the security device.
   - Enter the device admin name and password.
   - Select the connection method (Telnet, SSH version 1, SSH version 2) and the port number for the selected service.

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

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

5. After NSM autodetects the device, click **Next** to activate the device in NSM.

6. Click **Update Now** to update the configuration on the device with the settings from the modelled device. Or, you can click **Exit** to leave the wizard without updating the device.

**NOTE:** All passwords handled by NetScreen-Security Manager are case-sensitive.
If you do not update the configuration now, you will have to do it manually later 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.

**IDP Sensors**

To activate an IDP Sensor 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.

3. Select **Device Deployed and IP is Reachable**.

4. Click **Next** to display the Specify Connection Settings dialog box. Enter the connection information:
   - Enter the IP Address of the security device.
   - Enter the device admin name (admin).
   - Enter the device admin password.
   - Enter the device root password.

5. Click **Next** to display the Verify Device Authenticity dialog box.

6. Click **Next**.

7. Wait for the device to autodetect, then click **Next**.

8. After NSM autodetects the device, click **Next** to activate the device in NSM.

9. Click **Update Now** to update the configuration on the device with the settings from the modelled device. Or, you can click **Exit** to leave the wizard without updating the device.

If you do not update the configuration now, you will have to do it manually later by right-clicking the device and selecting **Update Device**.

---

**NOTE:** All passwords handled by NetScreen-Security Manager are case-sensitive.
Updating the device also pushes the Juniper Networks Recommended policy to the device.

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 **Activate Device**. The Activate Device wizard appears. Select **Device Deployed but IP is Not Reachable**.

3. Click Next to display the **Configure NACN and Global-PRO Logging** dialog box.
   - Enter the Serial Number of the device.
   - Enable Global-PRO logging to enable NetScreen-Security Manager to collect log entries from the device.
   - Enter the username and password of the device admin.

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

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

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

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

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

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

5. Click Finish to complete the Activate Device wizard.

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

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

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

**ScreenOS 5.x Devices**

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

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

2. Right-click the device and select **Activate Device**. The Activate Device wizard displays.

3. Select **Device Deployed but IP is Not Reachable**.

4. Click Next. Select Initialize Device Manually. (For details on initializing with a configlet, see “Using Rapid Deployment (ScreenOS only)” on page 113.)

5. Click Next.

   Specify the First Connection One Time Password (OTP) that authenticates the device.

NOTE: All passwords handled by NetScreen-Security Manager are case-sensitive.
Click Show Device Commands to display a list of CLI commands. The commands enable management and set the management IP address to the Device Server IP address, enable the Management Agent, set the Unique External ID, and set the device OTP.

Copy and paste these commands into a text file, then send the commands to the device administrator. The device admin must make a telnet connection to the physical device, paste the commands, and execute them to enable NetScreen-Security Manager management on the device.

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

6. Click Finish to complete the Activate Device wizard.

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 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.

IDP Sensors
To activate an IDP Sensor 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 Activate Device. The Activate Device wizard appears.

3. Select Device Deployed but IP is Not Reachable.

4. Click Next. Enter the device type and specify the OS version that is running on the device. Leave Support Level set on Full Support.

5. Click Next.

The wizard automatically enters the Unique External ID for the device. This ID number represents the device within the management system.
Chapter 4: Adding Devices

Specify the First Connection One Time Password (OTP) that authenticates the device.

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

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

6. Run the commands in the console of the device.

Send the commands to the device administrator. The device admin must make an SSH connection to the physical device, paste the commands, and execute them to enable NetScreen-Security Manager management on the device.

7. To check the device configuration status, mouseover the device in Device Manager (you can also check configuration status in Device Monitor):

- Before the device connects, the status displays Waiting for 1st connect, indicating that the management system is waiting for the device to connect. (This event occurs very quickly and might not display.)
- After the device connects, the status displays Import Needed, indicating that the device has connected but the management system has not imported the device configuration yet.

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

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

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.

Using Rapid Deployment (ScreenOS only)

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

- Simplify the deployment of firewall devices in non-technical environments
- Minimize device staging or technical staff required at deployment site
Enable secure and efficient deployment of a large number of firewalls

Bring new security devices under NetScreen-Security Manager management for initial configuration

NOTE: RD is supported on the following security devices: ns204, ns208, ns25, ns50, ns5Gt-Combined, ns5Gt-Dmz-Dual-Untrust, ns5Gt-Dual-Untrust, ns5Gt-Extended, ns5Gt-Home-Work, ns5Gt-Trust-Untrust, ns5GtAdsl-Extended, ns5GtAdsl-Home-Work, ns5GtAdsl-Trust-Untrust, ns5GtAdslWlan-Extended, ns5GtAdslWlan-Home-Work, ns5GtAdslWlan-Trust-Untrust, ns5GtWlan-Combined, ns5GtWlan-Dmz-Dual-Untrust, ns5GtWlan-Dual-Untrust, ns5GtWlan-Extended, ns5GtWlan-Home-Work, ns5GtWlan-Trust-Untrust, ns5XP, ns5XT-Combined, ns5XT-Dual-Untrust, ns5XT-Home-Work, ns5XT-Trust-Untrust, nsHSc-Home-Work, nsHSc-Trust-Untrust.

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

The **NetScreen-Security Manager administrator** works in the NetScreen-Security Manager UI. First, add a device to the UI, then creates a device configuration with specific or template-driven values. Next, enter the basic information that defines how a security device can contact your NetScreen-Security Manager Device Server and generate a small, static command file called a configlet. Save the configlet to a user-defined directory; using email, floppy disk, CD, or other out-of-band method, send the configlet file to the on-site admin that will be installing the configlet on the security device at its physical location. After the on-site admin installs the configlet and the device has successfully connected to the management system, you can install the modeled device configuration on the physical device.

The **On-Site administrator** works locally, at the physical device. At the security device, install the configlet on a locally-connected computer and run the Rapid Deployment Wizard. The RD wizard uses the information in the configlet to establish and authenticate a secure connection the NetScreen-Security Manager Device Server, enabling NetScreen-Security Manager to begin managing the device.

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

NOTE: If you delete the security device from the NetScreen-Security Manager system then re-add the device, you must also re-create the configlet and install on the physical device.

**Overview**

The NetScreen-Security Manager administrator adds a single device with RD in three stages:

1. Creating the Configlet
2. Installing the Configlet (performed by the on-site admin)
3. Updating the Device Configuration

The sections below detail each stage. For details on modeling, creating configlets for, and activating multiple devices at one time, see “Adding Many Devices (ScreenOS only)” on page 131.

Requirements

To use rapid deployment:

- The device must be running ScreenOS 5.x
- The device must use default factory settings.
- The device must be able to reach the Internet using a static IP address, a PPPoE- or PPPoA-assigned IP address, or DHCP-assigned IP address.
- The device must be modeled in NetScreen-Security Manager system. For details on modeling a device, see “Modeling a Device” on page 105

After you have modeled the device in the management system, you can begin tracking its status using the Device Monitor. Check the device configuration status by holding your mouse cursor over the device in Device Manager (you can also check configuration status in Device Monitor). The status should display **Modeled**, indicating that the management system has modeled the device, but the device is not activated and has not connected.

Creating the Configlet

After you have created a device configuration for the undeployed device, you are ready to activate the device and create the configlet.

1. Right-click the device and select Activate Device. The Activate Device wizard appears.
2. Select Device Deployed but IP is Not Reachable.
4. Click Next.
   - Specify the First Connection One Time Password that authenticates the device.

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

- The wizard automatically selects the interface on the device that will connect to the NetScreen-Security Manager management system. This interface is determined by the device platform and cannot be changed.
Select the Device Server connection. Use the default settings to configure the device to connect to the NetScreen-Security Manager Device Server IP address and port. Use a MIP to configure the device to connect to the NetScreen-Security Manager Device Server through a mapped IP address and port.

5. Click Next.

a. Specify the connection setting on the device:

- For devices with static IPs, you can pre-define the IP address, mask, and gateway OR ask the on-site admin to specify this information during configlet installation.

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

- For devices that use a PPPoE connection to the Internet, you can pre-define the user name and password OR ask the on-site admin to specify the user name and password during configlet installation.

---

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

---

- For devices that use a PPPoA connection to the Internet, you can pre-define the following ADSL parameters:

  - VPI/VCI Pair. The Virtual Path Identifier and Virtual Channel Identifier (VPI/VCI) identify the virtual circuit on the DSLAM.

  - Multiplexing Mode. Also known as the ATM encapsulation method, the multiplexing mode defines how the ADSL interface handles the multiple protocols on the virtual circuit. Your service provider must tell you the type of multiplexing used on the ADSL line:
    - Virtual Circuit (VC)-based multiplexing carries each protocol is carried over a separate ATM virtual circuit.
    - Logical Link Control (LLC) carries several protocols to be carried on the same ATM virtual circuit. This is the default option for the ADSL1 interface on the NetScreen-5GTADSL security device.

  - RFC1483 Protocol Mode. RFC 1483 describes methods of transporting bridged or routed protocol data units (PDUs) over AAL5 links:
    - Bridged PDUs do not require the overhead of IPSec processing, thus allowing more usable bandwidth to be available for data traffic. Because non-IPSec traffic is not secured at the IP packet layer, you should use this mode only with a private virtual circuit (the service provider assigns a static IP address for the ADSL interface).
- Routed PDUs enable the NetScreen-5GT ADSL device to exchange routing information with another router through the ADSL interface.

- ADSL Operating Mode. The operating mode defines the physical line attributes for the ADSL interface:
  - Auto Detect (default mode) enables the ADSL interface to automatically negotiate the operating mode with the service provider DSLAM.
  - ANSI T1.413 Issue 2 Mode
  - ITU G.992.1 Mode enables the ADSL interface to use the International Telecommunications Union (ITU) G.dmt standard, which supports minimum data rates of 6.144 Mbps downstream and 640 kbps upstream.
  - G.Lite Mode enables the ADSL interface to use the ITU 992.2 standard, which supports maximum data rates of 1.536 Mbps downstream and 512 kbps upstream.

Alternatively, you can prompt the on-site admin to specify these parameters during configlet installation.

- If you don’t know the ISP environment or the environment has location-specific networking requirements, prompt the on-site admin to configure the ISP environment during configlet installation.

b. Specify the password for the configlet, or use the default device password (which is netscreen).

c. Specify Device User Names and passwords, or use the default admin name and passwords for the device.

d. Restrict the use of the configlet to the current device. If checked, the configlet can only be installed on a device with the specified serial number.

6. Click Next to display the decoded configlet. To see the encoded configlet, click the Raw Configlet tab. Click Save to save the configlet (configlet files automatically use the format .cfg).

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.

---

**NOTE:** For security reasons, you cannot edit a configlet file directly. To make changes to the information in a configlet file, run the Activate Device wizard to re-generate the configlet.
To help the on-site admin through the configlet installation process, you should also send them the Rapid Deployment Getting Started Guide available on the Juniper Networks NetScreen-Security Manager Documentation CD. This guide provides step-by-step instructions for connecting a security device to the network, preparing the device to use a configlet, and installing and running the configlet.

The on-site admin must complete the configlet installation process and the device must successfully connect to the management system before you can update the device with the modeled configuration.

You can track the connection status of the device to determine when the device connects. Check the device configuration status by holding your mouse cursor over the device in Device Manager (you can also check configuration status in Device Monitor).

Before the device connects, the status displays **Waiting for 1st Connect**, indicating that the management system has modeled and activated the device, but the device has not connected.

After the on-site admin has installed the configlet, the device automatically connects to the management system and the status displays **Update Needed** indicating that the device has connected but the management system has not installed the modeled device configuration yet.

**Installing the Configlet**

The on-site admin performs RD in two stages:

- **Preparing the security device**
- **Installing the Configlet**

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

**Preparing the Device**

Before you install the configlet, you must prepare the security device:

1. Connect the device to your network. For details on connecting the device, see the User’s Guide that came with your security device.
2. Connect a standalone computer, such as a laptop, to the device **eth1** port.
   - To connect directly to the device, use a cross-over cable.
   - To connect to the device over a hub or switch, use a straight-through cable.

   If your device has auto-sensing ports, you can use any type of Ethernet cable to connect to the device.
3. Change the IP address of the standalone computer to 192.168.1.2 and the default gateway to 192.168.1.1. To change an IP address, see your computer’s operating system documentation.
4. Ensure that the device is using the factory default settings.
   - RD works with the factory default setting of all security devices running ScreenOS 5.x. If the device does not use the factory default settings, you cannot use RD (the WebUI cannot load the configlet).
   - To restore the factory defaults on the firewall device, see the User’s Guide that came with your security device.

5. Ensure that the Status LED on firewall device displays green.

Installing the Configlet

NOTE: During the configlet installation process, you cannot edit the device configuration.

To install the configlet:

1. Save the configlet on the standalone computer that you connected to the security device.

2. In a Web browser, enter the IP address of the trust interface on the security device as 192.168.1.1. The Rapid Deployment Wizard appears.

3. Select Load configlet file and browse to the location of the saved configlet file. Click Next.

   The RD Wizard opens the configlet, authenticates the integrity of the configlet, and decrypts the configlet. If the configlet is valid, the RD Wizard uses the configlet information to prepare the security device for NetScreen-Security Manager management.

4. If prompted, enter the configlet password and click Next. The configlet password is given to you by the NetScreen-Security Manager administrator who sent you the configlet file. Click Next.

5. Confirm or enter the ISP information. The ISP information describes the ISP environment in which the device is deployed. If the NetScreen-Security Manager administrator included ISP information in the configlet, the RD Wizard displays that information. Ensure that all information is correct.

   If the NetScreen-Security Manager administrator did not include ISP information or included only partial information, you must complete the ISP environment for the device:

   - If your firewall device uses DHCP to obtain an IP address from the network, select Using cable modem (Dynamic IP via DHCP).
   - If your firewall device uses a PPPoE connection to the Internet, select Using DSL modem (Dynamic IP via PPPoE). Enter the username and password for your PPPoE account.
   - If your firewall device uses a static IP address, select Using ISP-supplied Settings (Static IP) and enter the IP address, Netmask, and Gateway for the firewall device.
If your security device uses a PPPoA connection to the Internet (available on NetScreen-5GT ADSL devices), select PPPoA. Enter the multiplexing mode, VCI/VPI pair, Multiplexing mode, RFC1483 Protocol mode, and the ADSL operating mode for your PPPoA account.

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

The security device connects to the NetScreen-Security Manager Device Server. During this first connection, the device and the NetScreen-Security Manager Device Server exchange authentication information. After NetScreen-Security Manager authenticates the connection and saves the device public key, it sends a confirmation message to the device, which displays the message in the RD Wizard.

7. Click close to exit the RD Wizard.

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

---

**NOTE:** For security reasons, after the first successful connection, the security device erases the one-time-password (OTP) from memory.

---

**NOTE:** If the configlet installation process fails, you must reset the device to factory defaults. For details, see the User's Guide that came with the security device.

---

**Updating the Device Configuration**

After the on-site admin has installed the configlet and the device has successfully connected to management system, you can install the modeled device configuration on the physical device:

1. Ensure that the device is connected by viewing the device status. Check the device configuration status by holding your mouse cursor over the device in Device Manager (you can also check configuration status in Device Monitor). Ensure that the configuration status for the device displays **Update Needed**, which indicates that the device has connected but the management system has not updated the device configuration yet.

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

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

**Summarize Delta Config**

NSM now allows you to perform the command **Summarize Delta Config** on a device before you update the device. You can cancel the **Update Device** directive as well as save the **Summarize Config** output. The **Update Device** has the following two phases: Summarize Delta Config and Update Device.
Users can change the default to combine these two phases so that the delta config summary is automatically performed before the device is updated and the results are used to update the device as an optimization. During this combined operation, both results (Delta Config and Update Device) are available to you by selecting **View Device Delta Config**, if you have the appropriate admin rights. Otherwise, you can still update the device, but you cannot run **Summarize Delta Config**.

**EXAMPLE:** USER SELECTS SUCCESSFULLY UPDATE TWO DEVICES WITH DELTA OPTION
1. In the main navigation tree, select **Device Manager > Security Devices**.
2. From the menu bar, select **Devices > Configuration > Update Device Config** to open the **Update Device(s)** dialog box, listing all connected and managed devices.
3. Select two devices you want to update.
4. Select **Run Summarize Delta Config** (if deselected), then click **OK**.
   
   NSM displays the delta config results for both devices and both were successful.
5. Click **Update**.
6. Close the **Job Information** window and select **Job Manager** from the main navigation tree.
7. Select **Update Device** to see the update device job results for both devices.

**EXAMPLE:** USER SELECTS TWO DEVICES TO UPDATE WITH DELTA OPTION AND ONE DEVICE FAILS
1. In the main navigation tree, select **Device Manager > Security Devices**.
2. From the menu bar, select **Devices > Configuration > Update Device Config** to open the **Update Device(s)** dialog box, listing all connected and managed devices.
3. Select two devices you want to update.
4. Select **Run Summarize Delta Config** (if deselected), then click **OK**.
   
   NSM displays the delta config results. One device succeeded and the other device failed.
5. Click **Update**.
6. Close the **Job Information** window and select **Job Manager** from the main navigation tree.
   
   Only the device that passed delta config is updated.

**EXAMPLE:** USER SELECTS TWO DEVICES TO UPDATE WITHOUT THE DELTA OPTION
1. In the main navigation tree, select **Device Manager > Security Devices**.
2. From the menu bar, select **Devices > Configuration > Update Device Config** to open the Update Device(s) dialog box, listing all connected and managed devices.

3. Select two devices you want to update.

4. Deselect **Run Summarize Delta Config** (if selected), then click **OK**.

NSM displays the updated device job results for both devices.

**EXAMPLE:** USER SELECTS TWO DEVICES TO UPDATE WITH THE DELTA OPTION, BUT HAS NO ADMIN PRIVILEGES

1. In the main navigation tree, select **Device Manager > Security Devices**.

2. From the menu bar, select **Devices > Configuration > Update Device Config** to open the Update Device(s) dialog box, listing all connected and managed devices.

3. Select two devices you want to update.

4. Select **Run Summarize Delta Config** (if deselected), then click **OK**.

NSM displays the delta config results for both devices.

## Adding Other Device Types

You can also add or import other device types into NetScreen-Security Manager, including:

- Adding Vsyst Devices
- Adding an Extranet Device
- Adding a Cluster
- Adding a Vsyst Cluster and Vsyst Cluster Members

You cannot add multiple vsys, extranet, or cluster devices at one time; you must add each vsys, extranet, and cluster device (and cluster member) individually.

### Adding Vsyst Devices

A Virtual System (vsyst) is a virtual device that exists within a physical security device. The vsyst device functions as a completely separate security device. The physical device, called the root device, can contain multiple vsyst devices. The following Juniper Networks security devices can be root devices:

- NetScreen-500
- ISG-1000
- ISG-2000
- NetScreen-5200
NetScreen-5400

Placing the Root Device
Before you begin importing or modeling a root device, determine where you want to place the vsys devices:

- To add vsys devices in the global domain and one or more subdomains, add the root device to the global domain.
- To add vsys devices in a single subdomain, add the root device to that subdomain.

An example is shown below:

Figure 32: Connecting Vsys Devices Across Domains

[Diagram showing the placement of root and vsys devices across domains]

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”.

- **Import the vsys devices**—To import a vsys device, use the Add vsys wizard to add the vsys device. If you are adding multiple vsys devices to the same domain, you can add them all at once.

To import a vsys device:

1. From the domain menu, select the domain that contains the root device.
2. In Device Manager, click the Add icon and select vsys Device. The Add Device wizard appears.
   - Select the root device for the vsys.
   - Select a color to represent the vsys in the UI.
Select Import Existing Virtual System From Physical Device

3. Click Next. Select the domain in which to import the device.

4. Click Next. Select the vsys devices to import:
   - Use SELECT ALL to import all vsys devices from the root device.
   - Use SELECT NONE to clear all checked vsys devices.

5. Click Finish to complete the Add Device wizard. NetScreen-Security Manager automatically imports the select vsys configurations, and the new vsys devices appear in the Device Manager list.

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

To view the imported configuration, double-click the vsys in Device Manager.

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

**Modeling Vsys Devices**

Modeling vsys devices is a two stage process:

- Import or Model the root device—To import or model the root device, use the Add Device wizard to add the root device to the appropriate domain. For details, see “Importing Devices” on page 92 or “Modeling Devices” on page 104.

- Model the vsys device—To model a vsys device, use the Add vsys wizard to add the vsys device. You can model a vsys on an imported or modeled root device; however, you cannot update the vsys device configuration until you have first activated the root device. You must model one vsys device at a time.

To model a vsys device:

1. From the domain menu, select the domain that contains the root device.

2. In Device Manager, click the Add icon and select vsys Device. The Add Device wizard appears.
   - Select the root device for the vsys.
- Select a color to represent the vsys in the UI.
- Select Model Virtual System Device

3. Click Next to specify the Virtual System information:

- **NSM vsys Name.** Enter a name for the vsys device. This name identifies the vsys device in the NetScreen-Security Manager UI. The name can contain letters, numbers, spaces, dashes, and underscores.

- **ScreenOS vsys Name.** Enter a name for the vsys device. This name is stored in the root device. The name can contain letters and numbers and can be no longer than eight characters.

- **Domain.** Select the domain in which to model the device.

The wizard automatically complete the vsys ID, device type, and OS version of the root device.

4. Click Next to select the Virtual Router for this device:

- **Default Vrouter.** Use the default virtual router in the root device.

- **Shared Vrouter.** Select a one of the virtual routers defined in the root device to be shared with vsys devices.

- **User Vrouter.** Enter the name of a user-defined virtual router in the root device.

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

6. Ensure that the vsys is connected by viewing the device status. Check the configuration status by holding your mouse cursor over the device in Device Manager (you can also check configuration status in Device Monitor). Ensure that the configuration status for the vsys displays *Update Needed*, which indicates that the device has connected but the management system has not updated the device configuration yet.

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

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

After you have modeled the vsys device, create the vsys configuration and update the device. To check the vsys configuration status, mouseover the vsys device in Device Manager (you can also check configuration status in Device Monitor). The device status displays as **Managed**, indicating that the vsys has connected and the management system has successfully updated the vsys configuration.
Adding L2V Root Systems
The NetScreen-5000 series security devices running ScreenOS 5.0 L2V also support
vsys transparent mode, also known as layer 2 vsys, or L2V vsys. The VLAN Trunk
vsys mode and the L2V mode are mutually exclusive; you must enable one or the
other on the root system:

- When modeling an L2V root, ensure that the ScreenOS version is set to 5.0L2V
  and the operating mode is set to Transparent. By default, the root system is
  modeled as a neutral vsys, enabling you to configure the system in either L2V
  or VLAN Trunk mode.

- When importing an L2V root:
  
  - If the device is in transparent mode with L2V enabled, NetScreen-Security
    Manager imports those settings and creates the device in L2V mode.

  - If the device is transparent mode with L2V disabled, NetScreen-Security
    Manager creates the device in neutral vsys mode (you can use
    NetScreen-Security Manager UI to configure the device in VLAN or L2V
    mode).

  - If the device is transparent mode with VLAN trunk enabled,
    NetScreen-Security Manager imports those settings and creates the device
    in VLAN mode. In this mode, you can add vsys devices to the root system,
    but you cannot import VLAN IDs to those vsys devices.

For details on configuring these vsys modes, see “NetScreen-Security Manager:
Configuring Firewall/VPN Devices”.

Adding an Extranet Device
An extranet device is a firewall or VPN device that is not a security device. If you use
devices from multiple manufacturers, you can add extranet devices to
NetScreen-Security Manager to represent your heterogeneous network
environment. After you have added the extranet device to the NetScreen-Security
Manager UI, you can use the device in groups, Security Policies, and VPNs.

To add a new extranet device in Device Manager, click the add icon and select
Extranet device. The Extranet Device dialog box appears. Enter the extranet device
information:

- Name—Enter the name of the extranet device. The name can contain letters,
  numbers, spaces, dashes, and underscores.

- Color—Select the color that represents the extranet device in the
  NetScreen-Security Manager UI.

- IP Address—Enter the IP Address of the extranet device

Click OK to add the extranet device to NetScreen-Security Manager.
Adding a Cluster

A cluster is two security devices joined together in a high availability configuration to ensure continued network uptime. The two device configurations are synced, meaning both devices share the same configuration settings, enabling either device to handle traffic for the other if one device fails.

Adding a cluster is a two stage process:

1. Add the cluster device object.
2. Add the members of the cluster to the cluster device object. (When importing cluster members, ensure that their device configurations are in sync.)

Adding a Cluster Device Object

In Device Manager, click the Add icon and select Cluster. Enter the cluster information:

- **Cluster Name**—Enter a name for the cluster.
- **Color**—Select a color to represent the cluster.
- **Physical Choice**—Select the security device platform for both cluster members.
- **OS Version**—Select the OS version for both cluster members.
- **(ScreenOS only) Transparent Mode**—Enable transparent mode, if desired.

The cluster device object appears in the device tree.

Adding Members to the Cluster

Next, add the members of the cluster to the cluster device object. In Device Manager, right-click the Cluster device and select New > Cluster Member. The Add Device wizard appears; follow the instructions in the wizard to import or add a new cluster member.

- When importing cluster members, first ensure that their configurations are in sync. Next, use the Add Device Wizard to automatically import the device configurations from each physical cluster device member.
- When modeling a cluster member, ensure that both cluster members have been added to the cluster device object before configuring the cluster.

By default, the cluster propagates settings made in one device member to the other device member. However, the following settings are not propagated and must be configured on each device in the cluster: VSD group, VSD priority, authentication and encryption passwords, manage IP addresses, and IP tracking settings. All other commands are propagated among devices within the cluster.

For details on creating and configuring a cluster, see “NetScreen-Security Manager: Configuring Firewall/VPN Devices”. For example, to create a cluster that includes an existing device (with an existing configuration and Security Policy) and a new device (with no configuration or Security Policy), you should:
1. Create the cluster.

2. Add the existing device by importing. The Add Device Wizard automatically imports the device configuration.

3. Add the new device by modeling, then activating the device.

**Adding a Vsys Cluster and Vsys Cluster Members**

A vsys cluster is a vsys device that has a cluster as its root device. Adding a vsys cluster is a three stage process:

1. Add a vsys device that uses the cluster device as root. For details on adding a vsys device, see “Adding Vsys Devices” on page 122.

2. Add cluster members to cluster device, using the instructions in the wizard to import or add a new cluster member. A cluster can have only two members.

3. Add a cluster device object. For details on adding a cluster, see “Adding a Cluster” on page 127. (You add members later.)

The UI also creates a vsys cluster member for each vsys device that uses the cluster as its root device. The vsys cluster member contains local information; the cluster member contains the global information. Although a cluster can have only two members, a root vsys device can support more than two vsys devices.

**EXAMPLE: ADDING A VSYS CLUSTER**

In this example, you add a vsys cluster with two members and two vsys.

1. Add the cluster device:
   a. In the main navigation tree, select Device Manager > Security Devices. Click the Add icon and select Cluster. The new cluster dialog box appears. Configure as detailed below:
      - For Name, enter Paris Cluster.
      - For Physical Choice, select ns5400.
      - For OS Version, select 5.1.
   b. Click OK to save the new cluster object.

2. Add cluster members:
   a. In the main display area, right-click Paris Cluster and select New > Cluster Member. The New Cluster Member dialog box appears.
   b. Configure the cluster members OfficeA and OfficeB as shown below:
As you add each cluster member, NetScreen-Security Manager automatically creates both the cluster member and the vsys cluster member. In the security device tree, the Paris Cluster (and cluster members) and Paris vsys cluster (and cluster member) appear as shown below:
Paris Cluster Members and Paris Vsys Cluster Members

Add the first Vsys device:

a. Click the Add icon and select Vsys Device. The new Vsys device dialog box appears.

b. Configure the root as the Paris Cluster device, select a color, and choose Model Virtual System/Virtual System Cluster Device. Click Next to continue.

c. Configure the NetScreen-Security Manager and ScreenOS name as Paris V1, then select global as the domain. Click Next to continue.

d. Configure the vrouter for the vsys as the Default Vrouter, then click Next to continue.

e. Click Finish to add the new vsys cluster device.

3. Add the second vsys cluster device:

a. Click the Add icon and select Vsys Device. The new Vsys device dialog box appears.

b. Configure the root as the Paris Cluster device, select a color, then select Model Virtual System/Virtual System Cluster Device. Click Next to continue.

c. Configure the NetScreen-Security Manager and ScreenOS name as Paris V2, then select global as the domain. Click Next to continue.

d. Configure the vrouter for the vsys as the Default Vrouter, then click Next to continue.

e. Click Finish to add the new vsys cluster device.
The Paris Cluster and Paris V1 devices now appear in the security device tree.

Adding Many Devices (ScreenOS only)

If your network includes a large number of security devices, adding each device individually can take unwanted time and effort. To help you import or model your existing devices into NetScreen-Security Manager, you can now add multiple devices in a single workflow using the Add Many Device wizard.

With the wizard, you can add up to 4000 devices at a time to a single domain (you cannot add multiple devices to different domains at one time). Additionally, you can create configlets for and activate newly deployed security devices that are running ScreenOS 5.x; however you cannot configure Rapid Deployment when adding many security devices that are systems (NetScreen-500, NetScreen-5000, ISG 1000, ISG 2000).

NOTE: You cannot add Cluster or Cluster Members using the Add Many Device wizard.

Adding many devices is a three step process:

1. Create the CSV file. This file defines all the required and optional values for each device.

2. Using the Add Many Devices wizard, select the CSV file to import or model the devices. The wizard first validates the CSV file and notifies you of any errors, then adds the devices for which all defined values are valid.
   - When importing devices with static IP addresses, the device configuration is automatically imported during the Add Many Devices workflow.
   - When importing devices with dynamic IP addresses, you must manually import the device configuration after the Add Many Device workflow is complete.
   - When modeling ScreenOS 5.x devices for Rapid Deployment, you can also create configlets during the Add Many Devices workflow, or select to skip configlet creation.

   The time it takes for NetScreen-Security Manager activate and import devices depends on the number of devices and the management system configuration.

3. Verify the device configuration.

The following sections detail each step.
Creating the CSV File

Within a .csv file, you define the device configuration values for each device you want to add. The required and optional values depend on how the device is deployed on your network: static IP addresses, dynamic IP addresses, or undeployed devices.

NOTE: When adding security devices running ScreenOS 4.x that use NACN, you must specify the NACN interface (the interface that NetScreen-Security Manager uses to manage NACN).

You must create a separate CSV file for the following devices:

- **Devices with known IP addresses**—In this CSV file, you define the device parameters required to add and import the device configurations from ScreenOS 4.0.x and 5.x devices.

- **Devices with unknown IP addresses**—In this CSV file, you define the device parameters required to add ScreenOS 4.0.x and 5.x devices to the NetScreen-Security Manager system.

- **Undeployed devices**—In this CSV file, you define the device parameters required to add and model the devices in the NetScreen-Security Manager system.

NOTE: You can model many devices, but you cannot activate many devices except when using the Rapid Deployment process.

Juniper Networks provides csv templates in Microsoft Excel format for each type of csv file. These templates are located in the utils subdirectory where you have stored the program files for the UI client, for example:

C:\Program Files\NetScreen-Security Manager\utils

For each csv file, the header row defines the required and optional parameters; each subsequent row defines a single device’s values for those parameters. Columns are separated by commas.

**Devices with Static IP Addresses**

For devices with static IP addresses, create a .csv file with the following parameters:

**Table 13: CSV File Information for Devices with Static IP Addresses**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Type</th>
<th>Required</th>
<th>Acceptable Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>String</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>Color</td>
<td>String</td>
<td>yes</td>
<td>black, gray, blue, red, green, yellow, cyan, magenta, orange, pink</td>
</tr>
<tr>
<td>Device IP Address</td>
<td>String</td>
<td>yes</td>
<td>192.168.1.1, 10.1.1.10, 3.3.3.3</td>
</tr>
<tr>
<td>Device Admin Name</td>
<td>String</td>
<td>yes</td>
<td>&lt;admin&gt;</td>
</tr>
</tbody>
</table>
Chapter 4: Adding Devices

EXAMPLE: USING AN EXCEL FILE TO ADD MULTIPLE STATIC IP DEVICES

To view the template for adding many device with static IPs:

1. Download the Microsoft Excel file Add_Many_Devices_Reachable.xls from the Juniper Networks support Web site. The header row at the top defines the settings.

2. Using one row for each device you want to add, enter the required values for the device. You can also provide optional values, if desired.

3. Save the file to a location on your local drive.

EXAMPLE: USING A TEXT FILE TO ADD MULTIPLE STATIC IP DEVICES

To add two security devices that use static IP addresses, create a text file with the following text:

After you have created the file, save it as a .csv file.

Device with Dynamic IP Addresses

For devices with dynamic IP addresses, create a .csv file with the following parameters:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Type</th>
<th>Required</th>
<th>Acceptable Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Admin Password</td>
<td>String</td>
<td>yes</td>
<td>&lt; password&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Note: All passwords handled by NetScreen-Security Manager are case-sensitive.</td>
</tr>
<tr>
<td>Connection Protocol</td>
<td>String</td>
<td>yes</td>
<td>telnet, ssh_v1, ssh_v2</td>
</tr>
<tr>
<td>Device Admin Port</td>
<td>Integer</td>
<td>no</td>
<td>23, 22, 4444, 7777</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>If null, uses 23 for telnet and 22 for SSH</td>
</tr>
<tr>
<td>SSH Fingerprint</td>
<td>String</td>
<td>yes (when connection SSH)</td>
<td>&lt; SSH fingerprint&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>use any to bypass check</td>
</tr>
<tr>
<td>Global Pro Logging</td>
<td>String</td>
<td>yes</td>
<td>on, off</td>
</tr>
<tr>
<td>NACN</td>
<td>String</td>
<td>yes</td>
<td>on, off</td>
</tr>
<tr>
<td>NACN Interface Monitored</td>
<td>String</td>
<td>yes (when NACN is enabled)</td>
<td>must be a valid device interface</td>
</tr>
<tr>
<td>NACN Password</td>
<td>String</td>
<td>yes (when NACN is enabled)</td>
<td>must be a minimum of 9 characters</td>
</tr>
</tbody>
</table>

Chicago, green,10.100.31.78,netscreen,netscreen,ssh_v2,,any,on,off,, 
Memphis, orange,10.100.20.236,netscreen,netscreen,ssh_v2,,any,on,off,untrust,password, 
Columbus, red,10.100.20.200,netscreen,netscreen,telnet,,any,off,off,, 
Cincinnati, blue,10.100.20.237,netscreen,netscreen,ssh_v2,,any,on,untrust,pw-nacn, 

Adding Many Devices (ScreenOS only) ■ 133
**Table 14: CSV File Information for Devices with Dynamic IP Addresses**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Type</th>
<th>Required</th>
<th>Acceptable Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>String</td>
<td>yes</td>
<td>dev1, Chicago, NS-208</td>
</tr>
<tr>
<td>Color</td>
<td>String</td>
<td>yes</td>
<td>black, gray, blue, red, green, yellow, cyan, magenta, orange, pink</td>
</tr>
<tr>
<td>Device Platform</td>
<td>String</td>
<td>yes</td>
<td>ns5GT-Combined, ns5GT-Dual-Untrust, ns5GT-Trust-Untrust, ns5GT-Trust-Untrust-DMZ,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ns5GTdasi-Home-Work, ns5GTdasi-Trust-Untrust, ns5GTdasi-Trust-Untrust-DMZ, ns5XP,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ns5XT, ns5XT-Combined, ns5XT-Dual-Untrust, ns5XT-Trust-Untrust, ns25, ns50, ns100,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ns204, ns208, ns500, ns5200, ns5400, nsHSC-Home-Work, nsHSC-Trust-Untrust, nsISG1000, nsISG1000</td>
</tr>
<tr>
<td>ScreenOS Version</td>
<td>String</td>
<td>yes</td>
<td>5.x, 4.0.x</td>
</tr>
<tr>
<td>Transparent Mode</td>
<td>String</td>
<td>yes</td>
<td>on, off</td>
</tr>
<tr>
<td>License Key Model</td>
<td>String</td>
<td>yes</td>
<td>range of values defined in dcf file</td>
</tr>
<tr>
<td>First Conn OTP</td>
<td>String</td>
<td>yes</td>
<td>(when using ScreenOS 5.x)</td>
</tr>
<tr>
<td>Device Serial Number</td>
<td>String</td>
<td>yes</td>
<td>(when using ScreenOS 4.0.x)</td>
</tr>
<tr>
<td>NACN Interface</td>
<td>String</td>
<td>yes</td>
<td>(when using ScreenOS 4.0.x) must be a valid device interface</td>
</tr>
<tr>
<td>Global Pro Logging</td>
<td>String</td>
<td>yes</td>
<td>on, off</td>
</tr>
<tr>
<td>Device Admin Name</td>
<td>String</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>Device Admin Password</td>
<td>String</td>
<td>yes</td>
<td>must be a minimum of 9 characters</td>
</tr>
<tr>
<td>Telnet Port</td>
<td>Integer</td>
<td>no</td>
<td>if null, defaults to 23</td>
</tr>
<tr>
<td>SSH Port</td>
<td>Integer</td>
<td>no</td>
<td>if null, defaults to 22</td>
</tr>
</tbody>
</table>

**EXAMPLE: USING AN EXCEL FILE TO ADD MULTIPLE DYNAMIC IP DEVICES**
To view the template for adding many device with dynamic IPs:

1. Download the Microsoft Excel file Add_Many_Devices_Unreachable.xls from the Juniper Networks support Web site. The header row at the top defines the settings.

2. Using one row for each device you want to add, enter the required values for the device. You can also provide optional values, if desired.

3. Save the file to a location on your local drive.
EXAMPLE: USING A TEXT FILE TO ADD MULTIPLE DYNAMIC IP DEVICES

To add two security devices that use dynamic IP addresses, create a text file with the following text:

```
dev03,red,ns204,5.0,off,advanced,netscreen123,43042002000071,,off,netscreen-super,netscreen,,
dev04,green,ns500,5.0,off,advanced,netscreen123,10062002000039,,off,super-netscreen,netscreen,,
```

After you have created the file, save it as a .csv file.

Undeployed Devices

For undeployed devices (ScreenOS 5.x only), create a .csv file with the following parameters:

Table 15: CSV File Information for Undeployed Devices

<table>
<thead>
<tr>
<th>Field name</th>
<th>Type</th>
<th>Required</th>
<th>Acceptable Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>String</td>
<td>yes</td>
<td>valid character</td>
</tr>
<tr>
<td>Color</td>
<td>String</td>
<td>yes</td>
<td>black, gray, blue, red, green, yellow, cyan, magenta, orange, pink</td>
</tr>
<tr>
<td>Platform</td>
<td>String</td>
<td>yes</td>
<td>must be a device platform that supports ScreenOS 5.x and configlets (cannot be a ns5GTADSL device)</td>
</tr>
<tr>
<td>ScreenOS Version</td>
<td>String</td>
<td>yes</td>
<td>must be a ScreenOS 5.x device platform</td>
</tr>
<tr>
<td>Transparent Mode</td>
<td>String</td>
<td>yes</td>
<td>on, off</td>
</tr>
<tr>
<td>License Key Model</td>
<td>String</td>
<td>yes</td>
<td>range of values defined in dcf file</td>
</tr>
<tr>
<td>First Conn OTP</td>
<td>String</td>
<td>yes</td>
<td>must be a minimum of 9 characters</td>
</tr>
<tr>
<td>Connection Type</td>
<td>String</td>
<td>yes</td>
<td>static, pppoe, dhcp, prompt</td>
</tr>
<tr>
<td>Device IP Address</td>
<td>String</td>
<td>yes</td>
<td>(when connection type is static)</td>
</tr>
<tr>
<td>Device Netmask</td>
<td>String</td>
<td>yes</td>
<td>8, 24, 28, 32 Any valid netmask in CIDR format</td>
</tr>
<tr>
<td>Device Gateway</td>
<td>String</td>
<td>yes</td>
<td>(when connection type is static)</td>
</tr>
<tr>
<td>PPPoE User Name</td>
<td>String</td>
<td>yes</td>
<td>(when connection type is PPPoE)</td>
</tr>
<tr>
<td>PPPoE User Password</td>
<td>String</td>
<td>yes</td>
<td>must be a minimum of 9 characters</td>
</tr>
<tr>
<td>Configlet Password</td>
<td>String</td>
<td>no</td>
<td>default to a random string between 9 and 256 characters</td>
</tr>
<tr>
<td>Device Admin Name</td>
<td>String</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>Device Admin Password</td>
<td>String</td>
<td>yes</td>
<td>must be a minimum of 9 characters</td>
</tr>
<tr>
<td>Telnet Port</td>
<td>Integer</td>
<td>no</td>
<td>default to 23</td>
</tr>
</tbody>
</table>
EXAMPLE: USING AN EXCEL FILE TO ADD MULTIPLE MODELED DEVICES
To view the template for adding many modeled devices:

1. Download the Microsoft Excel file Add_Many_Devices_Model.xls from the Juniper Networks support Web site. The header row at the top defines the settings.

2. Using one row for each device you want to add, enter the required values for the device. You can also provide optional values, if desired.

3. Save the file to a location on your local drive.

EXAMPLE: USING A TEXT FILE TO ADD MULTIPLE MODELED DEVICES
To add and model three security devices, create a text file with the following text:

```plaintext
dev13, orange, ns5X0, 5.0, off, advanced, netscreen123, static, 10.10.30.5, 32, 10.10.30.1, , , 123456abc, netscreen, netscreen, ,
de14, green, ns50, 5.0, off, advanced, netscreen123, pppoe, , , root, netscreen, , netscreen, , 1netscreen, netscreen1, ,
de15, red, ns204, 5.0, off, advanced, netscreen123, dhcp, , , , , 2netscreen, netscreen2, ,
```

After you have created the file, save it as a .csv file.

**Validating the CSV file**

When you add the device, NetScreen-Security Manager validates the configuration information in the .csv file and creates a Validation Report. The report lists any incorrect or duplicate configurations, and indicates the exact line that contains invalid data.

**NOTE:** The Validation Report displays only the first error in the line. If the line contains additional errors, those errors do not appear in the Validation Report.

Select Cancel to quit the Add Many Devices process, or select Add Valid Devices to begin adding the devices for which you have provided valid device configurations. If the Validation Report listed incorrect configurations, you can still select Add Valid Devices; however, only the devices with correct configurations are added. If the .csv file contains duplicate configurations, NetScreen-Security Manager ignores the duplicates.

After you have added device, you cannot rollback or undo your changes. To edit or delete a device, select the device in the UI and make the necessary changes.

**Importing Many Devices**

The import process differs slightly between devices that use static IP addresses and devices that use dynamic IP addresses:
For devices with static IP addresses, the Add Many Devices wizard automatically imports the device configurations.

For devices with dynamic IP addresses, you must manually import the device configurations.

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

After you have added the devices, you should take a moment to verify that the device configuration import matches your expectations. For details, see “Verifying Imported Device Configurations” on page 102.

Adding Many Devices with Static IP Addresses

For devices with static IP addresses:

1. From the domain menu, select the domain in which to import the device.
2. In Device Manager, click the Add icon and select Many Devices. The Add Device wizard appears.
   - Select Device is Reachable (default).
   - Specify the location of the CSV file.
3. Click Next. The Add Device wizard validates the CSV file and provides a Validation Report:
   - Select Cancel to quit the Add Many Devices process.
   - Select Add Valid Devices to begin adding the devices for which you have provided valid device configurations.

The Add Device wizard adds the valid devices and automatically imports their configurations.

Adding Many Devices with Dynamic IP Addresses

For devices with dynamic IP addresses:

1. From the domain menu, select the domain in which to import the device.
2. In Device Manager, click the Add icon and select Many Devices. The Add Device wizard appears.
   - Select Device is Not Reachable.
   - Specify the location of the CSV file.
   - Specify the output directory for the .cli file. For each valid ScreenOS device configuration that uses a dynamic IP address, NetScreen-Security Manager creates a .cli output file. During the add process, you can specify the directory (Cli Server Output Subdir) that should be used to save the .cli file. By default, the .cli file is saved to the following GUI Server directory:
Before the device can be managed by NetScreen-Security Manager, you must enter the CLI commands in the .cli file on the physical security device.

3. Click Next. The Add Device wizard validates the CSV file and provides a Validation Report:
   - Select Cancel to quit the Add Many Devices process.
   - Select Add Valid Devices to begin adding the devices for which you have provided valid device configurations.

4. The Add Device wizard adds the valid devices and automatically imports their configurations.

Modeling Many Devices

For undeployed devices, you can create their device configurations in NetScreen-Security Manager in a single workflow. After you have created modeled configurations for each device, you must activate all devices individually.

To model many devices:

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

2. In Device Manager, click the Add icon select Many Devices. The Add Device wizard appears.
   - Select Model Device.
   - Specify the location of the CSV file.

3. Click Next. The Add Device wizard validates the CSV file and provides a Validation Report:
   - Select Cancel to quit the Add Many Devices process.
   - Select Add Valid Devices to begin adding the devices for which you have provided valid device configurations.

4. Model the device configuration as desired.

After you have added the device and created modeled device configurations for your undeployed device, you are ready to activate the device and prompt it to connect to the management system. After that device has made contact with NetScreen-Security Manager, you can install the modeled configuration you created on the physical device. For details on activating a device, see “Activating a Device” on page 106.
Using Rapid Deployment

You can model, generate configlets, and activate many ScreenOS 5.x devices at one time. Alternatively, you can choose to model multiple devices initially, then generate configlets and activate them at a later time. The devices must be running ScreenOS 5.x and support configlets; NetScreen systems (NetScreen-500, 5000 series, ISG 1000, and ISG 2000) do not support configlets.

Modeling and Activating Many Devices (with Configlets)

To model, create configlets, and activate at the same time:

1. From the domain menu, select the domain in which to import the device.
2. In Device Manager, click the Add icon and select Many Devices. The Add Device wizard appears.
   - Select Model Device.
   - Specify the location of the CSV file.
   - Select Activate and Create Configlets now (ns208 and below).
   - Specify the output directory for the .cfg file. For each modeled ScreenOS 5.x device configuration, NetScreen-Security Manager creates a .cfg output file. During the configlet creation process, you can specify the directory (Configlet Server Output Subdir) that should be used to save the .cfg file. By default, the .cfg file is saved to the following GUI Server directory:
     
     /usr/netscreen/GuiSvr/var/ManyDevicesOutput/<inputFile_YYYYMMDDHHMM>

3. Click Next. The Add Device wizard validates the CSV file and provides a Validation Report:
   - Select Cancel to quit the Add Many Devices process.
   - Select Add Valid Devices to begin adding the devices for which you have provided valid device configurations.

The Add Device wizard adds the valid devices to the NetScreen-Security Manager UI.

4. Send the .cfg file to the on-site administrator for the corresponding device. After the on-site administrator installs the configlet on the physical security device, the device automatically contacts the NetScreen-Security Manager Device Server, which establishes an always-on management connection. For instructions for the on-site administrator, see “Installing the Configlet” on page 118, or refer to the Rapid Deployment Getting Started Guide.

5. Model the device configurations as desired.

6. Install the modeled configuration. After the on-site administrators have installed the configlets and the devices have successfully connected to management system, you can install the modeled device configurations on the physical devices:
a. Ensure that the device is connected by viewing the device status. Check the
device configuration status by holding your mouse cursor over the device in
Device Manager (you can also check configuration status in Device
Monitor). Ensure that the configuration status for the device displays
**Update Needed**, which indicates that the device has connected but the
management system has not updated the device configuration yet.

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

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

For more details on the Rapid Deployment, see “Using Rapid Deployment
(ScreenOS only)” on page 113.

**Activating Many Devices (with Configlets)**

Before activating devices and creating a configlet, you must configure a modeled
configuration for the device in the NetScreen-Security Manager UI.

To create configlets and activate many devices:

1. In Device Manager, click the Add icon and select Activate Many Devices. The
   Activate Device wizard appears.

2. Select the devices to activate.

3. Specify the output directory for the .cfg file. For each modeled ScreenOS 5.x
device configuration, NetScreen-Security Manager creates a .cfg output file.
During the configlet creation process, you can specify the directory (Configlet
Server Output Subdir) that should be used to save the .cfg file. By default, the
.cfg file is saved to the following GUI Server directory:

   `/usr/netscreen/GuiSvr/var/ManyDevicesOutput/<inputFile_YYYYMMDDHHMM>/`

**NOTE:** For security reasons, you cannot edit a configlet file directly. To make changes to
the information in any configlet file, run the Activate Many Device wizard to
re-generate the configlets.

4. Send the .cfg file to the on-site administrator for the corresponding device. After
the on-site administrator installs the configlet on the physical security device,
the device automatically contacts the NetScreen-Security Manager Device
Server, which establishes an always-on management connection. For
instructions for the on-site administrator, see “Installing the Configlet” on
page 118, or refer to the Rapid Deployment Getting Started Guide.

5. Click OK. A Job Manager window appears to display the progress of the
activation. When completed, click Close.

6. Update the physical device with the modeled configuration.
Chapter 5
Configuring Devices

The Device Manager module in Juniper Networks NetScreen-Security Manager enables you to configure the managed Juniper Networks security devices in your network. You can edit configurations after you add or import a managed device, or create configurations when you model a device. For details about adding, importing, or modeling a device, see “NetScreen-Security Manager: Configuring Firewall/VPN Devices”.

This chapter details the device configuration parameters, and provides configuration examples when possible. For instructions for configuring specific device settings, see the NetScreen-Security Manager Online Help. This chapter also details two important tools that you can use to simplify configuring multiple security devices: templates and device groups.

This chapter contains the following sections:

- About Device Configuration on page 144
- Using Templates on page 149
- Using Device Groups on page 165
- Configuring Device Information on page 166
- About Device Configuration on page 144

After you edit or create a configuration for a device, you must update the configuration on the managed device for your changes to take effect. For details on updating devices, see “NetScreen-Security Manager: Configuring Firewall/VPN Devices”.

Use Security Policies to configure firewall and VPN rules that control traffic on your network, as described in Chapter 9, “Configuring Security Policies”. Use the VPN Manager to configure VPNs, as described in Chapter 10 “Configuring VPNs” or in “NetScreen-Security Manager: Configuring Firewall/VPN Devices”.


About Device Configuration

The device configuration contains the configuration settings for a managed device, such as interface, routing, and authentication settings. You can edit configurations after you add or import a managed device, or create configurations when you model a device. When you are satisfied with your changes, you can then update the managed device with the modeled device configuration to make your changes effective.

**NOTE:** When you open a device for viewing or editing, the NetScreen-Security Manager UI loads the entire device configuration into memory to enhance UI performance while configuring the device. When you close a device to which you made changes, the UI unloads some of the device configuration from the client memory. Although this memory optimization occurs quickly, you might see the following message appear: “Optimizing client memory usage for device”.

NetScreen-Security Manager does not support all device configuration settings. You may need to make some changes to the device directly using a Web UI or CLI. Additionally, some changes can affect the management connection between the NetScreen-Security Manager Device Server and the managed device.

About Configuring Security Devices

A security device provides perimeter and boundary protection using data encryption, authentication, access control, and some attack detection and prevention. Firewalls and virtual private networks (VPNs) are designed for high speed operation at the network layer.

While firewalls provide protection, there are attacks contained within the allowed traffic that firewalls are not designed to detect.

About Configuring IDP-Capable Devices

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

NetScreen-Security Manager is the sole means for configuring and managing IDP on the ISG 2000, ISG 1000, and standalone IDP Sensors running IDP 4.x. Standalone IDP Sensors running IDP 3.x and older are managed using the IDP Management Server and UI.

The ISG 2000 and ISG 1000 security module, an optional component installed in the device, provides IDP functionality. If you purchased a ISG 2000 or ISG 1000 device that does not have IDP capability, you can upgrade the device to be an IDP-capable system by replacing the memory chip in the CPU, installing up to three security modules, and installing the Advanced and IDP license keys for IDP.
About Configuring Extranet Devices

NetScreen-Security Manager also enables you to configure an existing extranet device (i.e., third-party router). You can do this by creating a script to perform the required actions on the extranet device. These scripts are saved by default on the GUI Server at:

GuiSvr/var/scripts

Add the extranet device in the Device Manager, then configure the required metadata in a shared object in the Object Manager under “Extranet Policies”. This data may include: credential info (user/password), IP, Interface List, comments, Action Script and other additional data. When you update the device, the specified script is invoked. The device update job displays the XML output.

EXAMPLE: CONFIGURING AN EXTRANET DEVICE

In this example, you want to update an existing rule on a third-party router to deny certain http traffic with integer fields matching 1-10.

This process involves first creating a script that updates the policy on the router. For example, the script can contain certain validation instructions for the policy. It can also include instructions on sending alerts or messages in the event that the policy update succeeds or fails. When you are done creating the script, save it in the appropriate directory.

Next, use the Object Manager to create a custom policy field object that contains the specific integer fields that you are referencing in the extranet policy (for example, integer fields matching 1-10).

To create a custom policy field:

1. In the Object Manager, select Custom Policy Fields.
2. In the Field Definition tab, click New. The New Custom Policy Fields Meta Data window appears.
3. Configure the Custom Policy Field:
   - Enter a name for the field, for example, call it ID.
   - Click the Required checkbox
   - Select Integer in the Type pull-down
   - Enter any appropriate Comments
   - Click OK. A folder for the ID custom policy field object appears.
5. Enter a value in the Data Value field, for example, enter 1. Click OK. The new value appears in the ID folder.
6. Repeat this step for all ten integer values.
In the Object Manager, create the Extranet Policy object with the appropriate rules.

To create an Extranet Policy object:

1. In the Object Manager, select Extranet Policies. The New ExtranetPolicyObject window appears.

2. Enter the name of the Extranet Policy, for example, Extranet Policy1. Add a comment in the Comments field.

3. Configure the Extranet Policy object:
   - Click New. The New - Rule window appears.
   - Use the up/down arrow to specify an ID for the rule
   - Add a comment for the rule
   - Click Deny in the Action field
   - Select a Source Address in the Source tab
   - Select a Destination Address in the Destination tab
   - Select in the Service tab
   - Select the integer IDs that you created in the Custom Policy Field object in the Options tab
   - Click OK.

Create the router as an Extranet Device in the Device Manager. You will need to configure the IP address of the device, any interfaces, then bind the extranet policy to the appropriate interface.

To create an Extranet Device:

1. In the **Device Manager**, select **Security Devices**.

2. Click New, and select Extranet Device. The New Extranet Device window appears.

3. Configure the Extranet Device:
   - Enter a name for the device, for example, Cisco Router1.
   - Select a color to represent the device.
   - Enter the IP Address for the device.
   - Click on the Show button in the Supplemental Data field. Additional fields appear allowing you to configure supplemental information for the device including the Netmask, Interface(s) and Device Root Admin.
   - Click New in the Interfaces field. The New Extranet Device Interfaces window appears.
Configure the Interface. Enter a name for the Interface, IP Address, Interface Mask, and assign an extranet policy to it, for example, the Extranet Policy1 object you configured previously. Click OK.

Configure the Device Root Admin. Enter the Admin User Name, Password, and specify the script you created previously in the Action field. Click OK.

When you update the device, NSM invokes the script you created. Any XML output appears in the Job Information window.

About Configuring Devices Running ScreenOS 5.0 FIPS
The following features are disabled on security devices running the Federal Information Processing Standards (FIPS) certified release of ScreenOS (ScreenOS 5.0FIPS):

- SNMP management
- MD5 algorithm use
- Group 5 Phase 2 IKE proposals

For more information about FIPS-enabled security devices, refer to the ScreenOS 5.0FIPS Reference Note.

NOTE: To configure and manage security devices running ScreenOS 5.0FIPS using NetScreen-Security Manager, you must first configure a VPN tunnel between the device and the NetScreen-Security Manager GUI Server. After establishing this tunnel, you can not reconfigure tunnel parameters in NetScreen-Security Manager.

About Configuring Devices Running Future Releases of ScreenOS
You can use NetScreen-Security Manager to configure security devices running future releases of ScreenOS in one of three levels of support:

- Forward Support (Basic)—when a new version of ScreenOS is available, you can download a schema patch which includes changes to the DCF and schema files, as well as the firmware tables, enabling you to manage devices using a previously known version of ScreenOS.

- Forward Support (Blended)—when a new version of ScreenOS is available, you can download a schema patch, enabling you to manage devices using the new ScreenOS version. You can not, however, manage the new features in ScreenOS with this level of support.

- Full Support—when a new version of ScreenOS is available, you can download a schema patch, enabling you to manage devices using the new ScreenOS version. In addition, you can also manage all the new features in that version of ScreenOS.

The Support Level is indicated in the Information screen for the device in the Device Manager.
Unsupported Changes

Some device configurations can be performed only by the device administrator using the CLI or WebUI. A NetScreen-Security Manager administrator cannot perform the following device configurations in the Device Manager:

- Configuring functions that are only applicable for the device administrator, such as setting initial IKE contact, audible alarms, MAC addresses, or console operations.
- Configuring functions that require device administrator intervention, such as Secure Command Shell (SCS) and Secure Shell (SSH) client operation.
- Executing debugging commands.

Changes that Affect the Management Connection

Some configuration changes to a managed device can affect the NetScreen-Security Manager connection to the device when you update the device, such as:

- Changing the connection method (Telnet or SSH) used between the NetScreen-Security Manager Device Server and the managed device.
- Disabling the ability of the managed device to communicate with the NetScreen-Security Manager Device Server.
- Changing the IP address of the NetScreen-Security Manager Device Server on the managed device.
- Changing the interface on the managed device that is permitted to receive NetScreen-Security Manager management traffic.
- Changing the VPN that handles traffic between the managed device and the NetScreen-Security Manager Device Server.
- Modifying router information on the managed device.
- Changing Security Policy rules on the managed device that cause NetScreen-Security Manager traffic to be dropped.

If you need to make any of the above changes to the managed device, use the WebUI or CLI to make the changes locally, then re-import the device configuration into the NetScreen-Security Manager UI.

Determining Device Configuration Status

You can view the connection and configuration status for each managed device in Device Manager.
NetScreen-Security Manager automatically updates the device status and displays the state of each device in the UI. To view device status, place your mouse cursor over the device name. A tooltip appears stating the device name, device type and ScreenOS version, IP address, domain, and the connection and configuration states.

NOTE: Detailed configuration status is not supported for devices running ScreenOS 4.0.x or 5.0.x.

Using Templates

Use templates to define a common device configuration and then reuse that configuration information across multiple devices. In a template, you can define only those configuration parameters that you want to set; you do not need to specify a complete device configuration. Templates provide two benefits:

- You can configure parameter values for a device by referring to one or more templates when configuring the device.
- When you change a parameter value in a template and save the template, the value also changes for all device configurations that refer to that template. See “Modifying Template Values” on page 159.

When you apply a template to a device, NetScreen-Security Manager applies the template settings to the device. For example, you can create a template that specifies the IP address of the NTP server to which all managed security devices synchronize their clocks. You can apply this template to the configuration of each device in your domain so that all devices use the same NTP server. You can apply the same template to different types of security devices, from NetScreen-5XT appliances to NetScreen-5200 systems.

A template contains all possible fields for all possible devices. Not all devices have all fields. You can apply a template to any device. NSM will ignore any fields that do not apply to the given device.

A template can refer to other templates, enabling you to combine multiple templates into a single template. When you make changes to any of the referenced templates, those changes are propagated through the combined template. For more information about the options you can configure, see the later sections in this chapter, starting with “Configuring Device Information” on page 166. For instructions for creating and applying templates, see the NetScreen-Security Manager Online Help topic, “Adding Device Templates” and “Applying Templates”.

Templates and Importing Devices

You can set device values via a template or directly on the device. If you import a device that already has certain values set, then those values are also stored by NSM. The interaction of templates and device values varies, depending on the sequence.

If you assign a template to a device before you import it’s values, then NSM looks to see which imported values match the template values. If a value matches, then NSM does not store the devices value; it just uses the value from the template. Then, if you change the value in the template, the value on the device will change as well.
If you import the device before assigning a template, then NSM will store the devices value, regardless of what value the template holds. If you change the template value, the value on the device will not change.

You can override device settings manually or by using the Template Operations dialog.

**Changing Values Set By Templates**

You can manually override any value set by a template in the individual device configuration. All fields set by templates appear in blue and have a template icon next to them. All fields that were set by a template but manually overridden have a red circle-and-slash icon over the template icon.

To determine which template set the value, move the mouse cursor over the field name:

- If the value is set by a template, the message “From: template-name” appears, as shown below:

![Figure 34: View Template Override Message](image)

- If the value is set by the individual device (a device-specific value), the template that was overridden appears.

For any value in the device configuration that was set by a template and overridden, right-click the value and select **Revert to template/default value** to revert the device-specific value to the template-defined value (this also reverts non-template values back to the default value). An example is shown below:
A device-specific configuration value always overrides a template value.

In addition, if a device has a policy set to none or Please select, templates will not override these values, since they are set by a user. You can remove these values with the procedure described above.

**Template Limitations**

When configuring and using templates in NetScreen-Security Manager, be aware of the following limitations.

**Maximum of 63 Templates**

You can apply a maximum of 63 templates to a single device. However, configuring certain features reduces the maximum number of templates you can apply to a device:

- **Cluster or vsys member**—Configuring a device as a vsys device or as a member of a cluster reduces the maximum number of templates by one.

- **VPNs**—Each VPN that the device belongs to also reduces the maximum number of templates by one. This includes VPNs configured in VPN Manager and VPNs configured at the device-level.

- **Referenced templates**—Each referenced template (a template referred to by another template) reduces the maximum number of templates by one. For example, a device that uses template A, which in turn refers to templates B and C, calculates three templates applied to the device.

**Device Groups**

You cannot apply a template to a device group. To use the same template for multiple devices, you must apply the template to each device individually.

**Default Values**

When creating a template, default values do not appear, as many default values depend on the Juniper Networks ScreenOS version and device platform.
Device Entities

Templates do not automatically include any of the entities that are predefined on devices, such as zones, interfaces, or virtual routers. To create a template that refers to a specific predefined entity, you must create the entity in the template.

For example, to create a template that refers to the ethernet1 interface:

1. In the template navigation tree, select **Network > Interface**.
2. Click the Add icon and select **Predefined Interface**. The Physical Interface dialog box appears.
3. For Name, enter ethernet1.

**NOTE:** When creating or editing predefined interfaces in a template, you must use full names for the interface (such as trust, untrust, ethernet1, ethernet1/2, and so on). Do not use names in short form, such as eth2/x instead of ethernet2/x.

When adding an entity in a template, ensure that the menu option you select is appropriate for the predefined entity. Choose the menu option that includes the name of the predefined entity you are creating.

For example, to create a template that refers to the mgt zone:

1. In the template navigation tree, select **Network > Interface**.
2. Click the Add icon and select **Predefined Functional Zone > mgt/vlan**. The Zone dialog box appears.
3. Enter mgt.

Key List Parameters

Key list parameters uniquely identify a configuration object in a list of similar objects and are read-only. You cannot edit key list parameters that are derived from a template. For example, a zone name uniquely identifies a zone in a list of zones that can be configured on a device. If you create a zone in a template and apply the template to a device, you cannot change the zone name in the device configuration. You must first delete the template-derived zone, then create a new zone.

A configuration object can contain multiple key list parameters. For example, in the routing table, multiple parameters (including IP address/netmask, interface, next-hop, vsys, and so on) uniquely identify a particular route entry.

**EXAMPLE:** CREATING A DEVICE TEMPLATE FOR DNS SETTINGS

In this example, you create a template that configures the IP addresses of primary and secondary DNS servers.

1. In the navigation tree, select **Device Manager > Security Device Templates**. Click the Add icon in the Device Template Tree or the Device Template List.

   The New Device Template dialog box appears, displaying the template navigation tree in the left pane and the Info screen in the right pane.
2. In the Info screen, enter DNS in the Name field.

3. From the template navigation tree, select **Network > DNS**. Configure the following:
   - For Primary DNS Server IP, enter 1.1.1.1.
   - For Secondary DNS Server IP, enter 2.2.2.2.
   - For DNS Refresh Schedule, select **Refresh Daily**. Leave all other default settings.

4. Click **OK** to save the template. You can now use this template when configuring security devices.

**EXAMPLE: APPLYING A DEVICE TEMPLATE**

In this example, you apply the DNS template you created in the previous example:

1. Ensure that the device you want to apply the template to has been successfully added to the management system.

2. In the navigation tree, select **Device Manager > Security Devices**, then double-click the device to open the Device dialog box.

3. In the device navigation tree, select **Info > Templates**. The templates configuration screen appears.

4. Click the Edit icon. The Edit Templates dialog box appears.

5. Select the **DNS** template.

6. Click **OK** in the Edit Templates dialog box, then click **OK** to save your changes to the device configuration.
The Template Operations Dialog

Figure 36: Template Operations Dialog

Template Operations Dialog Controls

The Template Operations dialog is divided into the following four sections:

Select Devices section
In this section, select one or more devices for template operations.

Select Template section
Select one or more templates to apply to the selected devices. Use the edit button to bring up the Select Templates dialog. Check one or more checkboxes to select templates. Once you have selected templates and closed the Select Templates dialog, use the up and down arrow buttons to order the selected templates as you wish.
Template Operation section
The next section features four radio buttons, as follows:

- **Add templates with lowest priority**—Adds the templates to each device’s template list with the lowest priority. Added templates will be lower priority than templates previously assigned to the device. Templates with higher priority can override the values applied by these templates.

- **Add templates with highest priority**—Adds the templates to each device’s template list with highest priority. Added templates will be higher priority than templates previously assigned to the device. Values in these templates will override values applied by lower priority templates.

- **Remove templates**—Removes all selected templates from each selected device.

- **Don’t change templates**—Makes no changes to devices in database. This setting is useful if you want perform a validation, run a report, or clear overrides without changing the template assignments.

Options section
The last section provides optional operations, as follows:

- **Remove conflicting device values**—overrides any device settings that override template values provided by the selected templates. Normally, template values do not override manually set values.
- **Report irrelevant template values**—reports any values that are set in templates but that are not used on the selected devices. A template may provide values for features that aren’t available on every device. For example, wireless configuration information is not relevant to devices that do not provide wireless functionality.

**NOTE:** If the template specifies a field that a device does not support, the field does not appear in the Device dialog box and is not applied to the device. No validation message appears. You can see these values by checking the Report irrelevant template values checkbox.

If the template specifies a field that the device supports, but the value is outside the permitted range for the device, a validation message appears in the Device dialog box.

- **Report conflicts with other templates**—reports any values that conflict between the selected templates and existing templates assigned to the device. If there are undesired conflicts, you may need to modify the templates to get the configuration you want.

- **Validate**—checks that the configured device (after any changes) is a valid configuration and reports any errors.

**Using the Template Operations Dialog**

The Template Operations dialog allows you to add templates to devices, remove templates from devices, and validate device configurations after any changes.

**NOTE:** The Template Operations Dialog only updates the configuration database. To apply changes to devices, you must use the update directive.

The Template Operations dialog can be used in many ways. This section describes one recommended workflow.

**Step 1:** Look at the effect of planned changes before making them

1. Select **Devices > Configuration > Template Operations**.

2. Select one or more devices to validate templates against. 
   Example: 5gt, 5gt-12, 5gt-13, 500, 520, 1000

3. Select the Edit Templates button to bring up a list of templates.

4. Select one or more templates to validate against the devices. 
   Example: VPN, DNS, Route-Basic, Zone-Basic, admin-1

5. Click **OK**.

6. If you have selected more than one template, use the up and down arrow buttons to sort the templates. Templates higher in the list will be assigned first. Templates lower in the list will be assigned later. Later templates can override the settings of earlier templates.

7. Select the Don’t change templates radio button.
8. If you want, you can select one or more of the following validation and reporting options.

- **Report irrelevant template values (optional)**—reports template settings that are not relevant to the selected device or devices.

- **Report conflicts with other templates (optional)**—reports settings that conflict between two or more templates.

- **Validate (recommended)**—validates the device configuration after appropriate changes to the templates and the removal of conflicting values (if needed).

- **Do not select** Remove conflicting device values as it may alter device values.

9. Click OK.

**Step 2: Review results in job information dialog**

Consult the reports and error messages generated in Step 1. Resolve any conflicts, missing assignments, or other errors as desired. If desired, repeat steps 1 and 2 until you are satisfied with your planned changes.
Step 3: Apply templates and clear overrides

This procedure updates the NetScreen-Security Manager database, but does not push the new settings to the device.

CAUTION: You can easily reverse adding templates, but there is no automatic way to restore conflicting device values that have been removed. Be careful not to override values you want to keep.

Repeat the operations specified in Step 1, but specify one of the Add templates radio buttons. If desired, also check the Remove conflicting device values checkbox.

Removing Templates with the Template Operations Dialog

To remove one or more templates from one or more devices, select Devices > Configuration > Template Operations.

1. Select one or more devices to remove templates from.
   Example: 5gt

2. Select the Edit Templates button to bring up a list of templates.

3. Select one or more templates to remove.
   Example: DNS

4. Click OK.

5. Select the Remove templates radio button.

6. Click OK.

Templates and Validation

You can apply a single template to different device types that run different ScreenOS versions. In some cases, the field values you specify in the template might not be appropriate for all ScreenOS versions and device types:

- If the template specifies a field that a device does not support, the field does not appear in the Device Edit dialog box and is not updated to the device. No validation message appears.

- If the template specifies a field that the device supports, but the value is outside the permitted range for the device, a validation message appears in the Device dialog box. A template value may be valid for one device but invalid for other devices.

As you create and edit template values and fields, NetScreen-Security Manager performs validation, and might display validation messages. For example, you can configure an IP address in one template and the netmask for that IP address in another template. However, a validation message might appear when you enter the IP address because the netmask is not specified within that same template.

You can safely ignore a validation message if the missing value is derived from another template that is applied to the device, or if you manually entered in the value in the specific device configuration.
Modifying Template Values

You can modify a template that has already been applied to one or more device configurations. When you change a field value in a template, the new value appears in the device configuration the next time you edit the configuration. To change the field value on the device, you must update the device (see NetScreen-Security Manager Administrator’s Guide).

When you change a template, the configuration of one or more devices that use the template might become invalid. For example, a template change could cause a required field to be cleared or a field value to be outside the permitted range.

For instructions for modifying a template, see the NetScreen-Security Manager Online Help topic, “Editing Device Template”.

Applying Multiple Templates

When applying multiple templates to a single device, you determine the order that the templates are applied. The highest priority template is positioned at the end of the template list, and can override values set in any of the lower priority templates. If more than one template specifies a value for the same field, the value in the highest-priority template takes precedence. The lower the template appears in the template list, the higher priority it has when applying values to a device configuration.

EXAMPLE: USING MULTIPLE DEVICE TEMPLATES

In this example, you create two templates that each configure different values for the same firewall SCREEN option for the untrust zone. The first template, DoS, sets several values in the SCREEN options, including setting the source-based IP session threshold limit to 128 for the untrust zone. The second template, DoS2, sets the source-based IP session threshold limit to 256 for the untrust zone. When you apply these templates to a device, the template with the highest priority overrides the values in the lower priority template.

1. Create a template that sets SCREEN options for the untrust zone then apply the template to a NetScreen-208 device running Screen 4.0:
   a. In the navigation tree, select Device Manager > Security Device Templates and click the Add icon. The New Device Template dialog box appears.
   b. In the Info screen, enter DoS in the Name field.
   c. In the template navigation tree, select Network > Zone. The Zone configuration screen appears.
   d. Click the Add icon in the Zone configuration screen and select Predefined Security Zone. The Predefined Zone dialog box appears.
   e. In the General Properties screen, enter untrust in the Name field.

NOTE: Because the untrust security zone is predefined for the device, you must select the Predefined Security Zone option. You can select the Security Zone or Tunnel Zone option only when adding or configuring a user-defined zone.
f. In the zone navigation tree, select **Screen > Denial of Service Defense.** The Denial of Service Defense screen appears.

g. Select and configure the following options, then click **OK:**

- Select **SYN-ACK-ACK Proxy Protection** and set the Threshold to **512.**
- Select **Source IP Based Session Limit** and set the Threshold to **128.**
- Select **Destination IP Based Session Limit** and set the Threshold to **4000.**

h. Click **OK** to save the new device template.

2. Apply the DoS template to a device configuration for a NetScreen-208 running ScreenOS 4.0:

a. Add a NetScreen-208 security device to the management system, and model the configuration. Be sure to configure the device as running ScreenOS 4.0.

b. In the navigation tree, select **Device Manager > Security Devices.** Double-click the NetScreen-208 device icon to open the Device dialog box.

c. Select **Info > Templates** in the device navigation tree. Click the Edit icon in the Templates screen. The Edit Templates dialog box appears.

d. Select the **DoS** template.

e. Click **OK** in the Edit Templates dialog box.

3. Verify that the DoS template values have been applied to the device:

a. Select **Network > Zone** in the device navigation tree. Double-click the untrust zone. The untrust-Predefined Zone dialog box appears.

b. Select **Screen > Denial of Service Defense** and review the values applied by the template, as shown in Figure 39.
4. Create a second template that sets a different value for a SCREEN option than was set in the DoS template:

   a. In the navigation tree, select **Device Manager > Security Device Templates** and click the Add icon. The New Device Template dialog box appears.

   b. In the Info screen, enter **DoS2** in the Name field.

   c. In the template navigation tree, select **Network > Zone**. The Zone configuration screen appears.

   d. Click the Add icon in the Zone configuration screen and select **Predefined Security Zone**. The Predefined Zone dialog box appears.

   e. In the General Properties screen, enter **untrust** in the Name field.

   f. In the zone navigation tree, select **Screen > Denial of Service Defense**. The Denial of Service Defense screen appears. Select and set the Source IP Based Session Limit Threshold to **128**.

Your settings appear as shown in Figure 40.
g. Click OK in the Predefined Zone dialog box, then click OK in the New Device Template configuration dialog box.

5. Apply the DoS2 template to the NetScreen-208 device:
   a. In the navigation tree, select Device Manager > Security Devices. Double-click the NetScreen-208 device icon to open the Device dialog box.
   b. Select Info > Templates in the device navigation tree. Click the Edit icon in the Templates configuration screen. The Edit Templates dialog box appears.
   c. Select the DoS2 template.
   d. Click OK in the Edit Templates dialog box.

6. Set the template priority.

Currently, the DoS template has the highest priority, which enables it to override any similar values set by the DoS2 template, as shown in Figure 41.

Figure 41: View Template Priority (DoS Highest)

To set the DoS2 template to the highest priority, select the DoS2 template and click the down arrow icon above the list of templates (or press Alt-N.) The DoS2 template now has the highest priority, as shown in Figure 42.
Chapter 5: Configuring Devices

Figure 42: Set Template Priority (DoS2 Highest)

<table>
<thead>
<tr>
<th>Templates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Values from templates \textit{lower} in the list override values from templates \textit{higher} in the list.</td>
</tr>
<tr>
<td>DoS (Lowest Priority)</td>
</tr>
<tr>
<td>DoS2 (Highest Priority)</td>
</tr>
</tbody>
</table>

The DoS2 template now overrides similar values set in the DoS template.

7. Verify that the configuration values from the DoS and DoS2 templates have been applied in the device configuration:

   a. Select \textbf{Network} > \textbf{Zone} in the device navigation tree. Double-click the untrust zone. The untrust-Predefined Zone dialog box appears.

   b. Select \textbf{Screen} > \textbf{Denial of Service Defense} and review the values applied by the template, as shown in Figure 43.

Figure 43: View Values from DoS and DoS2 Templates

Although both the DoS and DoS2 templates configured threshold values for the Source IP Based Session Limit field, the higher threshold value from DoS2 appears in the device configuration because you assigned the DoS2 template a higher priority than the DoS template.

   c. Verify the origin of each value by pressing the Shift key and moving the mouse cursor over the field name.

For the Source IP Based Session Limit, the message “From template: DoS2” appears, as shown below:
Figure 44: View DoS2 Value for Source IP Based Session Limit

For the SYN-ACK-ACK Proxy Protection, the message “From template: DoS” appears, as shown below:

Figure 45: View DoS Value for SYN-ACK-ACK Proxy Protection Setting

8. Manually override the SYN-ACK-ACK Proxy Protection value that is set by the template DoS:
   b. Select and set the SYN-ACK-ACK Proxy Protection threshold to be 1000.
   c. 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, as shown below:

Figure 46: View Default SYN-ACK-ACK Proxy Protection Setting

Exporting and Importing Device Templates

Templates can be exported to a text file, then re-imported into another template. When an exported template is imported into a template, the values in the exported template overwrite existing values.

The exported template contains only device settings. It does not contain any policies or objects.

Exporting a Device Template

To export a device template, select Devices > Configuration > Export Device Template Config To File. When you see the file generated in the Job Information dialog, select Save Selected and give the file a name. You do not have to highlight the config file text. You can use any file extension.
Importing a Device Template

To import device template configurations into a template, select **Devices > Configuration > Import Device Template Config From File**. Then, select the templates you want the saved template settings to be applied to. Then, select the saved template you want to import. The settings in the saved template are imported into the NSM template.

Refer to the NSM Online Help for detailed procedures.

Using Device Groups

Use device groups to organize your managed devices, making it easier for you to configure and manage devices within a domain. You can group devices by type (such as all the NetScreen-5Gts in a domain), by physical location (such as all the security devices in the San Jose office), or logically, (such as all the security devices in sales offices throughout western Europe.)

Groups enable you to execute certain NetScreen-Security Manager operations on multiple security devices at the same time. For example, if you have a group of the same type of devices running similar ScreenOS versions, you can upload the firmware on all devices in the group at the same time. You can also add devices to the NetScreen-Security Manager UI, place the devices in a group, and then import the device configurations for all devices in the group at one time.

The devices that you add to a group must exist; that is, you must have previously added or modeled the devices in the domain. You can group devices before configuring them. You can add a device to more than one group. You can also add a group to another group.

**NOTE:** You cannot apply a template to a group. You must apply templates to individual devices in a group. If you need to apply the same set of templates to multiple devices, you can create a single template that includes all the templates that are to be applied to a device, and then apply the combined template to each device.

**EXAMPLE: CREATING A DEVICE GROUP**

In this example, you create a device group that includes security devices used to protect the Sales and Marketing department of your organization.

1. **Add and model the following devices to the management system:**
   - Outside Sales
   - Marcom
   - Direct Marketing
   - Sales
   - Marketing

2. In the navigation tree, select **Device Manager > Security Devices**.
3. Click the Add icon. The New Group dialog box appears, displaying all existing devices for the current domain in the Non-members list.

4. For **Name**, enter Sales.

5. In the non-members list, select the devices that you want to be part of the Sales device group.

6. Click **Add⇒** to move the selected devices to the Member list. Click **OK**.

### Configuring Device Information

To configure a device that has been added, imported, or modeled in NetScreen-Security Manager:

1. In the navigation tree, select **Device Manager > Security Devices**.

2. Open the device configuration using one of the following methods:
   - Double-click the device object in the security device Tree or the security device List.
   - Select the device object and then click the Edit icon.
   - Right-click the device object and select **Edit**.

   The device navigation tree appears on the left, listing the device configuration parameters by function.

3. In the device navigation tree, select a function heading to see device parameters, then select the configuration parameter you want to configure.

4. Make your changes to the device configuration, then choose one of the following:
   - Click **OK** to save your changes and close the device configuration.
   - Click **Apply** to save your changes and continue making changes.
   - Click **Cancel** to discard all changes and close the device configuration.

This section describes the Info options in the Device dialog box. Subsequent sections describe other options in the Device dialog box.

When you add or model a device in the NetScreen-Security Manager UI, you provide information about the device name, color, type, and OS version. If you imported the device configuration, the Info options display additional information about the device:

- **Info**—specifies the device name and the color that you have chosen to display the device in the NetScreen-Security Manager UI.
Device Type—specifies the type of security device that you are managing, including the version of ScreenOS that you are running on the device. Note that two types of OS Version now appear on the device:

- Managed OS Version refers to the version of ScreenOS that is supported by NetScreen-Security Manager
- Running OS Version refers to the actual version of ScreenOS running on the device - this may be a future version of ScreenOS not yet fully supported by NetScreen-Security Manager

Support Level indicates whether or not features on the device are either “Fully Supported” in which case you can use NetScreen-Security Manager to manage all the functionality in that version of ScreenOS, or “Forward Supported”, in which case you can use the Supplemental CLI to facilitate support of new features in ScreenOS. For more details on using Supplemental CLI, see “NetScreen-Security Manager: Configuring Firewall/VPN Devices”.

Other information including the Serial Number, IP Address and whether or not you are running the device in Transparent Mode is also provided.

- Device Root Admin—specifies the username and password of the root admin on the device
- NSM Connection—specifies the type of connection that NetScreen-Security Manager is using to connect to the device.
- Policy for Device—specifies the name of the policy that you are using to configure traffic on the device.

**Configuring Startup Information**

For modeled devices, and for imported devices that use a dynamic IP address, you must configure Startup information. The startup information includes the One-Time-Password (OTP) and the Device Server parameters.

**NOTE:** Certain encrypted passwords/keys are not imported into NetScreen-Security Manager including the OTP, root admin password, and wireless ssid psk-key and passphrase. If any of the above passwords/keys are changed out of band, then you must copy and save the encrypted value of the password/key using NetScreen-Security Manager. This enables you to avoid resetting the previous configured value upon next update. Other passwords and keys such as the “non-root admin” passwords are imported into NetScreen-Security Manager.

The OTP is used to authenticate the first connection communication between the physical device and NetScreen-Security Manager. The OTP is deactivated (unavailable) when:

- You have already set the OTP. After you have configured an OTP, you cannot reset it.
- For imported devices that use a static IP address. Because first connection communication occurs during the add device process, the OTP is not used and is deactivated by default.
For devices running ScreenOS 4.x. These devices do not use an OTP

Use the Device Server parameters to specify the primary and, if available, the secondary Device Server IP addresses and ports that manage the security device.

Applying Templates

You can set most device configurations, except policies and VPNs, in a template. You can also manually override any value set by a template.

The order in which the templates are listed determines how template values are applied to the device. When a value is set in more than one template applied to a device, the value in the highest-priority template takes precedence. To reorder templates, click the up or down arrow icon above the list of templates to move the priority up (lower priority) or down (higher priority). (Or, press Alt-U or Alt-N to move the priority of the template up or down.)

For more information about templates, see “Using Device Groups” on page 165.

Viewing Device Capabilities

The Capabilities screen lists features and resources available on the device. This screen is read-only; you cannot change any of the values on the screen.

The configuration screens that you see for a particular security device depend upon the following:

- Device platform
- ScreenOS version running on the device
- License key(s) installed on the device

Therefore, some of the configurations described in this chapter only apply to specific security devices, ScreenOS versions, or license key installations.

Configuring IDP Sensor Global Settings

Use Global Settings to specify syslog and SNMP servers.

In device templates, find these settings under IDP Device Settings. In an individual device, find these settings under Global Settings.

Syslog Server

To have all IDP logs sent to a Syslog server, enable the checkbox and specify the syslog server’s IP address, then load the new configuration onto the Sensor.

SNMP Server for Health Monitoring Alerts

The IDP Sensor creates and sends a log entry whenever one of the following statistics reaches 90%. It also sends a log when the value drops below 90%. Logs are sent no more than once a minute. The log entry specifies the value of the setting at the time the log is sent.
- **CPU Usage**—log entry generated when CPU usage reaches 90%.
- **Hard Disk Usage**—log entry generated when disk space reaches 90%.
- **Memory Usage**—log entry generated when memory usage reaches 90%.
- **Session Count**—log entry generated when session count reaches 90% of the total possible session count. (Maximum total session count for each device is specified on that device's product sheet.)

These logs are generated and sent to NSM automatically. However, you can also tell the Sensor to send the entries to your SNMP server. To do so, enable SNMP and specify the server’s community and IP address, then load the new configuration onto the Sensor.
Chapter 6
Updating Devices

This chapter details how to update the running configuration (the configuration on the security device) with the modeled configuration (the configuration in the Juniper Networks NetScreen-Security Manager UI). In addition to covering the basic update process, this chapter also details the events that can require you to update your device, as well as NetScreen-Security Manager tools that help you to track, verify, and preview the update process.

After you model or make changes to a device configuration in the NetScreen-Security Manager UI, you must install that device configuration on the physical Juniper Networks security device before those changes can take effect. For devices running ScreenOS 5.x, NetScreen-Security Manager supports atomic configuration, a fail-safe feature that ensures successful updates occur without errors or the update is not performed. Atomic configuration is always enabled and occurs automatically when a device update causes the device to lose its connection to the management server.

This chapter contains the following sections:

- About Updating on page 172
- Knowing When to Update on page 177
- Using Preview Tools on page 181
- Delta Configuration Summary Example on page 185
- Performing an Update on page 185
- Tracking Device Updates on page 188
About Updating

When you updated a managed device, you are modifying the running device configuration (the configuration currently installed on the physical device) with the modeled device configuration (the configuration currently modeled in NetScreen-Security Manager).

You can update a single device, multiple devices, vsys devices, clusters, and/or device groups simultaneously. For example, if you have created a device group that includes only NetScreen-5GT devices, you can update the entire device group in a single update procedure. During the update, NetScreen-Security Manager displays the progress of the update on each individual device so you can see exactly what is happening. Simultaneous updating also reduces downtime to unaffected devices and areas of your network.

Updating a device is a simple three-step process.

1. Ensure that you have configured the device correctly, created and assigned a policy to the device, and have established a connection between the device and the management server.

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

   - All connected and managed device appear in the device list. Modeled devices, or devices awaiting import for the first time do not appear.

   - For devices running ScreenOS 5.1 or higher, the configuration status also appears next to the device name. For more details on configuration states, see “Configuration Status” on page 178.

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

NetScreen-Security Manager uses centralized control and tracking to indicate when you need to update a device, and to follow the progress of the device configuration you are updating. Before updating your managed devices, you can use other NetScreen-Security Manager modules and tools to identify devices that need to be updated, validate their modeled configurations, and preview how those devices accept the new configuration. After updating, you can use those same tools to verify a successful update. These tools include:

   - Audit Log Viewer—This NetScreen-Security Manager module records changes made to a device configuration. The audit log entry also details the administrator performed the change, when the change was updated on the device, and a history of change details.

NOTE: Although atomic configuration provides fail-safe methods of protecting your ScreenOS 5.x devices from invalid configurations, you should be confident about the modeled configuration before updating the device.
Report Manager—This NetScreen-Security Manager module collects data from traffic logs on various events that occur over your network and provides a visual representation of them. You can customize reports to display and filter parameters.

Configuration Summaries—These tools provide a preview of the modeled configuration, enabling you to compare it with the configuration that is running on the device. Use configuration summaries to ensure the modeled configuration is consistent with what you want to update on the device.

Job Manager—This NetScreen-Security Manager module tracks the status of running and completed update processes. The Job Manager displays details of the update process in a dedicated information window and includes the update’s success or failure and errors involved in a failed update.

The Update Lifecycle

The lifecycle of the update process:

1. The managed device is functioning normally. You have successfully added the device to NetScreen-Security Manager, reviewed the device configuration, and updated the device. Suddenly, an event occurs on the managed device that requires a change to the device configuration. For example, malicious traffic might have entered your network, causing you to update the Security Policy for the device to detect and prevent that attack.

2. You locate the cause of the event. Using NetScreen-Security Manager modules such as the Realtime Monitor and Log Viewer, you determine the exact attack that penetrated the device. From the Report Manager, you also determine what rule in the Security Policy was ineffective in blocking the attack. You then update the modeled device configuration, editing the Security Policy to detect and prevent the attack from entering your network again.

3. (ScreenOS only) Before updating the running configuration, you review the modeled device configuration. Using a delta configuration summary, compare the modeled configuration with the running configuration on the device to confirm the differences. Fine-tune the modeled configuration, if needed.

4. When you are confident that the modeled configuration is valid, update the device. NetScreen-Security Manager updates the running configuration with only the new changes (delta); During the update, you track the update progress using Job Manager. In the job information window, you can track the progress of the update real-time and observe the transfer of the configuration from NetScreen-Security Manager to the device.

   If the update is unsuccessful, use the information in the Job information window to correct the problems in the modeled configuration.

5. (ScreenOS only) After updating, run a second Delta Configuration Summary to identify any remaining differences between the modeled configuration and the running configuration on the device. When the Delta Configuration Summary reveals no differences between the new configuration and the old configuration on the device, you have successfully updated the running configuration.
About Atomic Configuration (ScreenOS 5.x Only)

NetScreen-Security Manager uses atomic configuration, a fail-safe feature for security devices running ScreenOS 5.x. Atomic configuration ensures a current valid configuration is not overwritten by a flawed configuration in flash memory. The update must complete without errors and the device connection to the management system must remain active, or the update is aborted to prevent an invalid, error-prone, or flawed configuration to install on the device.

Atomic configuration is always on. During an update:

1. NetScreen-Security Manager saves and locks the active configuration on the device, then starts a timer for the update process. While the active configuration is locked, it cannot be saved.

2. NetScreen-Security Manager sends the modeled configuration to the device.

3. As the device receives the modeled configuration, it updates its existing active configuration with each command as the command is received:
   - If the device executes the entire modeled configuration (all commands) and the connection to the management system remains up, NetScreen-Security Manager unlocks the active configuration and saves the new active configuration.
   - If the device cannot execute a command, NetScreen-Security Manager resets the device, unlocks the active configuration, and restores the saved active configuration to the device (the device reboots). After rebooting, the device sends a final error message to the management system; this contents of this message, which include any CLI errors in the failed configuration, appear in the Job Manager status window for this update.
   - If the device connection to the management system is down after all commands have been executed, the update timer expires and the device automatically resets. The device unlocks the active configuration and restores the saved active configuration (the device reboots). The connection might be down due to a command in the modeled configuration that causes the device to lose connection with the NetScreen-Security Manager Device Server.

NOTE: When updating vsys devices, atomic configuration occurs only for the root vsys.

About Atomic Updating (ScreenOS 5.1 or Higher Only)

In addition to atomic configuration, devices running ScreenOS 5.1 and higher also support atomic updating, which enables the device to receive the entire modeled configuration (all commands) before executing those commands (instead of executing commands as they are received from the management system). Because NetScreen-Security Manager sends all commands at one time, the performance of the management connection is enhanced.
Atomic updating also enables the device to temporarily lose connection to NetScreen-Security Manager during the update process. If the management connection is down when the device has completed executing the commands in the modeled configuration, the device reestablishes the connection. Because the device no longer needs to maintain a constant connection to the management system during updating, you can configure changes to management connection from the NetScreen-Security Manager UI.

During an atomic update:

1. NetScreen-Security Manager saves and locks the active configuration on the device, then starts a timer for the update process (timeout: two hours). While the active configuration is locked, it cannot be saved.

2. NetScreen-Security Manager sends the modeled configuration to the device.

3. The device receives all commands before executing the commands on its existing active configuration. During the update, the device sends progress messages to the management system every 15 seconds; these messages appear in the Job Manager status window for the update.

During the update, the Job Manager status window displays other messages, depending on the success of the update:

- **Updates Without Errors**—If the device executes the entire modeled configuration (all commands) and the connection to the management system remains up or can be reestablished, NetScreen-Security Manager unlocks the active configuration and saves the new active configuration. The device sends a final message to the management system; this message appears in the Job Manager status window for this update.

- **Updates With Errors**—If the device cannot execute a command, it notifies the management system, which makes a decision whether to ignore and proceed, abort, or revert.
  - For ignore and proceed decisions, the device continues the update.
  - For abort and revert decisions, the device automatically resets. The device unlocks the active configuration and restores the saved active configuration (the device reboots). After rebooting, the device sends a final error message to the management system; this message, which includes any CLI errors in the failed configuration, appears in the Job Manager status window for this update.

- **Re-establish Management Connection**—If the device connection to the management system is down after all commands have been executed, the device attempts to reestablish connectivity.
  - If successful, NetScreen-Security Manager unlocks the active configuration and restores the saved active configuration to the device. The device sends a final message to the management system; this message appears in the Job Manager status window for this update.
If attempts to reconnect are unsuccessful for two hours, the update timer expires and the device automatically resets. The device unlocks the active configuration and restores the saved active configuration (the device reboots). After rebooting and reestablishing connection to the management system, the device sends a final error message to the management system; this message, which includes any CLI errors in the failed configuration, appears in the Job Manager status window for this update.

Retrying a Failed Update

When updating your managed security devices, the update fails for each device that is not connected to the management system at the time of update. For device running ScreenOS 5.1 and higher, you can configure NetScreen-Security Manager to save the pending changes for an unconnected device, then install those changes when the device finally connects to the management system.

NetScreen-Security Manager automatically changes the configuration state of an unconnected device that is waiting for changes to the “Sync Pending” state. When a device in this state connects to the management system, pending changes are immediately installed on the device and the configuration state is changed to “In-Sync”.

You can also configure the management system to abort update attempts for previously unconnected devices to which out-of-band changes have been made. For example, you attempt to update all your managed NS-5GT security devices, but device NS-5GT-25 is disconnected from the management system for troubleshooting at the time of update. When troubleshooting is complete and the device reconnects, to prevent NetScreen-Security Manager from overwriting any out-of-band changes made, enable the option “Don’t Update If Device Has Changed”.

Configuring Update Options

You can configure device update and retry options on a system-wide basis (in the UI preferences), on a per-update basis for multiple devices (in the device update dialog box), and on a per-update basis for a single device (in the device options dialog box). The system-wide settings appear as the default settings for the both per-update settings, which you can change as needed for each update.

When configuring system-wide update options, you can enable or disable any option independently; when configuring per-update options, dependencies apply.

Update options include:

- Rematch, Session Treatment when modifying a policy rule—When enabled, NetScreen-Security Manager preserves the existing sessions that are being tracked by the installed Security Policy during the policy update procedure (devices running ScreenOS 5.1 or higher only). At the end of the update, NetScreen-Security Manager restores all valid sessions on the managed device and deletes all invalid sessions.

When disabled, NetScreen-Security Manager does not preserve and restore existing sessions for a updated managed device.
Show Unconnected Devices in Device Selection Dialog—When enabled, the NetScreen-Security Manager UI displays devices that are not connected to the management system in the Update Devices dialog box (which displays when you attempt to update the configuration for a managed device).

When disabled, unconnected devices do not appear in the Update Devices dialog box, preventing admins from selecting an unconnected device for updating.

When configuring this option on a per-update basis, you must enable this option before the “Update When Device Connects” option is available.

Update When Device Connects—When enabled, NetScreen-Security Manager attempts to update a previously unconnected device with pending changes stored in the management system.

If you do not select this option, NetScreen-Security Manager attempts to update the device, but fails because the device is unreachable. The failed attempt is listed in the Job Manager.

When configuring this option on a per-update basis, you must enable this option before the “Don’t Update If Device Has Changed” option is available.

Don’t Update If Device Has Changed—When enabled, NetScreen-Security Manager does not update a previously unconnected device if out-of-band changes have been made to the device. The configuration state of the device appears as “NSM and Device Changed”, or “Device Changed” when the update device job is cancelled due to any change on the device.

Enable Option Dialog—When enabled, NetScreen-Security Manager displays device update options for single-device updates. The update options dialog box appears when you right-click a device in Device Manager and select Update Attacks.

When disabled, the update options dialog box does not appear for single-device updates initiated from the Device Manager. Alternatively, to disable from within the per-update device update dialog box, select the option “Don’t Show This Dialog”.

Knowing When to Update

You might need to update a device configuration for one or more reasons. Typically, you update a device after changing the device configuration or after modifying the Security Policy that is assigned to the device.

To overwrite the existing configuration on the physical device, update the physical device with the modeled configuration in NetScreen-Security Manager.

To overwrite the modeled configuration in NetScreen-Security Manager, import the existing configuration from the physical device. Currently, NetScreen-Security Manager does not support delta updates from the device.
Using NetScreen-Security Manager, you can identify the changes made to the device or to the modeled configuration, then update the device. For significant changes to the network that the security device is deployed in, you might also need to change the assigned policy.

Check the following areas to detect configuration or policy changes:

- Verifying Device Status in Device Monitor
- Verifying Device Status in Device Manager
- Reviewing Logs
- Identifying Administrative Changes
- Reviewing Reports

**Verifying Device Status in Device Monitor**
Within the management system, a managed device has an associated connection state and configuration state. NetScreen-Security Manager displays each status for each managed device in RealTime Monitor > Device Monitor.

For more details on using the Device Monitor, see “Monitoring Security Devices” on page 517.

**Connection Status**
The connection state indicates the status of managed device–Device Server connection. NetScreen-Security Manager uses heartbeat packets to continually test the connection between the Device Server and the physical device, and the connection status column in the Device Monitor displays the current status of the device:

- **Up status**—Indicates the device is connected to the Device Server and is running properly. Before you can update a device, it must be in the Up state.

- **Down status**—Indicates that an event has occurred, either manually by an administrator or automatically by the flow of a type of traffic, that has stopped the device from running.

- **Never Connected status**—Indicates that the device has not made an initial connection to Device Server. Typically, this state appears for modeled devices that have not been activated, or for devices waiting to be activated using Rapid Deployment.

**Configuration Status**
The configuration state indicates the status of the device configuration on the physical device. Some common configuration states:

- **Managed**—Indicates that the running configuration is the same as the modeled configuration (the device is using a “managed” configuration).
- Modeled—Indicates that the running configuration is not the same as the modeled configuration, and that the device has not yet connected to NetScreen-Security Manager.

- Import Needed—Indicates that the running configuration is not the same as the modeled configuration, but the device has connected to NetScreen-Security Manager and is awaiting manual import (this configuration status occurs only when adding devices running ScreenOS 5.x to the management system).

- Update Needed—Indicates that the running configuration is not the same as the modeled configuration, and that the device is connected to NetScreen-Security Manager. You must update the managed device before the changes you made in the modeled configuration can take effect.

For devices running ScreenOS 5.1 and higher, NetScreen-Security Manager supports additional configuration states that indicate the status of the physical device configuration in relation to the modeled configuration in NetScreen-Security Manager. In addition to the states listed above, a device running ScreenOS 5.1 and higher can have one of the following four configuration states:

<table>
<thead>
<tr>
<th>Detail State</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managed, In Sync</td>
<td>The physical device configuration is synced with the modeled configuration in NetScreen-Security Manager.</td>
</tr>
</tbody>
</table>
| Managed, Device Changed | The physical device configuration is out-of-sync with the modeled configuration in NetScreen-Security Manager. Changes were made to the physical device configuration (the configuration on the physical device is newer than the modeled configuration).
To correctly synchronize the two configurations, import the configuration from the physical device. |
| Managed, NSM Changed    | The modeled device configuration is out-of-sync with the physical device configuration. Changes were made to the modeled configuration (the configuration on the NetScreen-Security Manager is newer than the physical device configuration).
Any change made in the UI automatically causes the NSM configuration state to change, even when the change is canceled or undone. For example, if you change a value in the UI to a different value, then undo the change by entering the original value, the NSM configuration state is still considered out-of-sync with the physical device.
To correctly synchronize the two configurations, update the configuration on the physical device. |
| Managed, NSM and Device Changed | Both device configurations (physical and modeled) are out-of-sync each other. Changes were made to the physical device configuration and to the modeled configuration. Although you cannot sync delta changes, you can run a delta config summary (see “Using a Delta Configuration Summary (ScreenOS only)” on page 182) to identify the differences, then manually make the changes to the modeled configuration and update the device. |
| Managed, Sync Pending   |                                                                         |

Changing the name, color, or NetScreen-Security Manager port on a device causes the configuration state to be out of sync, even though the management system and device do not share these parameters (these parameters are not transmitted to or from the device during an update).
For details on all states, see “Viewing Device Status” on page 517.

**Verifying Device Status in Device Manager**

You can view the connection and configuration status for each managed device in Device Manager.

NetScreen-Security Manager automatically updates the device status and displays the state of each device in the UI. To view device status, place your mouse cursor over the device name. A tooltip appears stating the device name, device type and ScreenOS version, IP address, domain, and the connection and configuration states.

To manually verify the configuration status for devices running ScreenOS 5.1 and higher:

- For a single device—Right-click the device and select Check Config Sync Status. This option appears only for devices running ScreenOS 5.1 and higher.
- For multiple devices—From the menu bar, select Devices > Configuration > Check Config Sync Status. Select the devices running ScreenOS 5.1 and higher for which you want to view configuration status, then click OK.

**NOTE:** You can use the directive Check Config Sync Status from any location in the NetScreen-Security Manager UI. (You do not need to have Device Manager selected.)

**Reviewing Logs**

The Log Viewer can help you identify event patterns on your network. To clarify the pattern in the Log Viewer, create a custom view using filters that display log entries based on specific criteria. To set a column or cell filter, right-click the column or cell that you want to use as the matching criteria and specify the value.

For example:

- To track all events for a specific time period, create a filter on the timestamp column; when applied, the filter displays only the log entries that meet the specified time period.
- To track all events from a specific source IP address, create a filter on source address column; when applied the filter displays only the log entries that use the specified source address.
- To track all events for a specific category or subcategory of log entries, such as Configuration or Attack log entries, create a filter on the category or subcategory column; when applied the filter displays only the log entries with the specified category or subcategory designation.

For more details on using the Log Viewer, see Chapter 14, “Logging”. For step-by-step instructions on creating a filter, see the NetScreen-Security Manager Online Help topic “Setting Filters”.
Identifying Administrative Changes

Use the Audit Log Viewer to identify administrative changes made to your managed devices. Audit log entries also detail the administrator who made the change, the action performed, and the date and time of the change. You can track changes by time of logging, administrator name, action, targets, and devices. If an administrator made a change to a device or an object, you might want to update the affected devices.

For details on using the Audit Log Viewer, see “Using the Audit Log Viewer” on page 631.

Reviewing Reports

Use Report Manager to determine when you are receiving too many attacks of a certain type and order them by an IP address. For example, if you determine that the current device configuration and Security Policy cannot block scans, you might want to create a new rule in the Security Policy that guards against those attacks, then update the device.

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

- To identify common events, select an event-based report to see the frequency of events in bar graph or pie chart. To see details for a specific event, right-click the event and select View in Log Viewer to display a custom view in a new window. You can save a detailed view as a custom report. For example, when viewing the Top Alarms, expand a location to view the data that makes up this location.

- To examine how specific rules in your Security Policy are performing, select the Administrative > Top Rules report. You might need to fine-tune an inefficient rule to better handle events in your network traffic.

For details on using Report Manager, see Chapter 15, “Reporting”.

Using Preview Tools

When you update a managed device, you are overwriting the existing configuration that is running on the physical device. Therefore, it is important to verify a configuration before sending it to the device.

Using preview tools, you can preview how the modeled configuration looks in CLI command form to predict the success of the update and anticipate errors.

NetScreen-Security Manager supports three types of preview tools:

- Configuration Summary—Displays the modeled configuration using ScreenOS CLI commands.

- Delta Configuration Summary(ScreenOS only)—Displays the modeled configuration and running configuration using ScreenOS CLI commands, and lists the differences between the two configurations.

- Running Config—Displays the configuration installed on the physical device.
The configuration and delta configuration summaries help you ensure that the modeled configuration is correct before you update your managed devices, while the running config helps you identify settings already on the managed device.

Running a Configuration Summary

When you update a managed device using NetScreen-Security Manager, the management system generates ScreenOS CLI commands that map to the settings in the NetScreen-Security Manager UI. To verify the configuration you are installing on the device generates the correct CLI commands, run a configuration summary.

1. From the file menu, select Devices > Configuration > Summarize Config. NetScreen-Security Manager displays the Get Configuration Summary dialog box.

2. Select the devices or device groups for which you want to run a Configuration Summary and click OK. A Job Information window appears to help you track the progress of the summary.

3. When the job completes, review the CLI commands in the Job Information window. When you update the device, these are the commands that NetScreen-Security Manager uses to overwrite the running configuration.

For some settings, the CLI commands for a UI settings do not map one-to-one. For example, a single vsys configuration in the NetScreen-Security Manager UI generates multiple ScreenOS commands.

Because the management system generates all information (UI settings and CLI commands) for a configuration summary, you can run a configuration summary on a modeled device (the device does not need to physically exist).

Using a Delta Configuration Summary (ScreenOS only)

A Delta Configuration Summary compares the active configuration on the device with the modeled configuration in NetScreen-Security Manager and displays the differences between the two configurations. The Delta Configuration Summary produces four sets of data.

<table>
<thead>
<tr>
<th>Delta Config Data</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config on Device but not on NSM</td>
<td>Displays the CLI commands detected on the device that do not map to NetScreen-Security Manager settings. Use this information to identify any out-of-band updates (made by the local device admin) to the running configuration; you might not want to overwrite these settings.</td>
</tr>
<tr>
<td>Config on NSM but not on Device</td>
<td>Displays the CLI commands (as mapped to NetScreen-Security Manager settings in the modeled configuration) detected in NetScreen-Security Manager but not on the device. Use this information to identify the changes you have made to the modeled configuration since the last update.</td>
</tr>
</tbody>
</table>
Chapter 6: Updating Devices

You should run a Delta Configuration Summary two times:

- Before updating—Because you are overwriting the running configuration with the modeled configuration, you might want to identify and verify the configuration you are installing on the device.

- After updating—Ensure that the device received the configuration as you expected, and that no differences exist between the running configuration and the modeled configuration.

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

To run a Delta Configuration Summary:

1. From the file menu, select Devices > Configuration > Summarize Delta Config. NetScreen-Security Manager displays the Get Delta Config Summary dialog box.

2. Select the devices or device groups for which you want to run a Delta Config Summary and click OK. A Job Information window appears to help you track the progress of the summary.

3. When the job completes, review the CLI commands in the Job Information window. Specifically, review the commands in the section “Config to be sent to device on next Update Device”; when you update the device, these are the commands that NetScreen-Security Manager uses to overwrite the running configuration.

An example Delta Configuration Summary is shown below:

<table>
<thead>
<tr>
<th>Delta Config Data</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config on both NSM and Device but reordered</td>
<td>Displays the CLI commands for configuration settings present on both the device and NetScreen-Security Manager, but the CLI command sequence has been reordered.</td>
</tr>
<tr>
<td>Config to be sent to device on next Update Device</td>
<td>Displays the CLI commands that NetScreen-Security Manager will send to the device on the next update.</td>
</tr>
</tbody>
</table>
Figure 47: Delta Configuration Summary Example

<table>
<thead>
<tr>
<th>Commands for objects already configured on the device</th>
</tr>
</thead>
<tbody>
<tr>
<td>unset interface serial manage telnet</td>
</tr>
<tr>
<td>unset interface serial manage web</td>
</tr>
<tr>
<td>unset interface serial manage ssl</td>
</tr>
<tr>
<td>unset interface serial manage snmp</td>
</tr>
<tr>
<td>unset interface serial manage scs</td>
</tr>
<tr>
<td>unset interface serial manage ping</td>
</tr>
<tr>
<td>unset av http trickling</td>
</tr>
<tr>
<td>set av all max-connections 0</td>
</tr>
<tr>
<td>set zone untrust screen syn-flood</td>
</tr>
<tr>
<td>set zone untrust screen syn-flood alarm-threshold 512</td>
</tr>
<tr>
<td>set zone untrust screen syn-flood attack-threshold 200</td>
</tr>
<tr>
<td>set zone untrust screen syn-flood queue-size 1024</td>
</tr>
<tr>
<td>set zone untrust screen syn-flood timeout 20</td>
</tr>
<tr>
<td>set zone untrust screen syn-flood source-threshold 512</td>
</tr>
<tr>
<td>set zone untrust screen syn-flood destination-threshold 1024</td>
</tr>
<tr>
<td>set policy id 1 from trust to untrust Any Any ANY permit</td>
</tr>
<tr>
<td>set nsrp ha-link probe threshold 5</td>
</tr>
<tr>
<td>set nsrp ha-link probe interval 1</td>
</tr>
<tr>
<td>set nsrp vsd-group init-hold 5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Commands for Objects configured in NetScreen-Security Manager.</th>
</tr>
</thead>
<tbody>
<tr>
<td>set pppoe name untrust</td>
</tr>
<tr>
<td>set zone untrust screen syn-flood</td>
</tr>
<tr>
<td>set zone untrust screen syn-flood alarm-threshold 512</td>
</tr>
<tr>
<td>set zone untrust screen syn-flood attack-threshold 200</td>
</tr>
<tr>
<td>set zone untrust screen syn-flood queue-size 1000</td>
</tr>
<tr>
<td>set zone untrust screen syn-flood timeout 20</td>
</tr>
<tr>
<td>set zone untrust screen syn-flood source-threshold 512</td>
</tr>
<tr>
<td>set zone untrust screen syn-flood destination-threshold 1000</td>
</tr>
<tr>
<td>set policy id 7000029 from trust to untrust Any Any ANY permit</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Commands on the device and NetScreen-Security Manager that have been reordered.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config on both Device and NSM but reordered:</td>
</tr>
<tr>
<td>set pppoe name untrust</td>
</tr>
<tr>
<td>set zone untrust screen syn-flood</td>
</tr>
<tr>
<td>set zone untrust screen syn-flood alarm-threshold 512</td>
</tr>
<tr>
<td>set zone untrust screen syn-flood attack-threshold 200</td>
</tr>
<tr>
<td>set zone untrust screen syn-flood queue-size 1000</td>
</tr>
<tr>
<td>set zone untrust screen syn-flood timeout 20</td>
</tr>
<tr>
<td>set zone untrust screen syn-flood source-threshold 512</td>
</tr>
<tr>
<td>set zone untrust screen syn-flood destination-threshold 1000</td>
</tr>
<tr>
<td>set policy id 7000029 from trust to untrust Any Any ANY permit</td>
</tr>
</tbody>
</table>
Occasionally, the delta configuration report might display discrepancies that do not actually exist between the running configuration and the modeled configuration. In some specific situations, the running configuration includes CLI commands that do not appear as pending changes in NetScreen-Security Manager, yet the two configurations are actually in sync (no deltas exist). This can occur when:

- Some settings for a feature have been configured in NetScreen-Security Manager, but the feature itself is not enabled. For example, if you configure NSRP settings but do not deploy the device in NSRP mode, the CLI commands for NSRP settings appear in the running configuration but are not managed by NetScreen-Security Manager (because the feature is not active).

- DHCP settings, such as interface IP addresses, are not assigned by NetScreen-Security Manager, and are not included in the CLI commands sent to the device. The CLI commands do appear, however, in the running configuration.

- Default, unconfigured settings might not be managed NetScreen-Security Manager. For example, if the running configuration includes the domain name mycompany.net, but that domain name is not configured in NetScreen-Security Manager, the management system leaves the value unchanged.

Performing an Update

You can update a single device, multiple devices, or device groups using the same process.

Before updating:

- Ensure that you have configured the device correctly, created and assigned a policy to the device, and have established a connection between the device and the management server.
- Run a Configuration Summary on the device to view the CLI commands for the modeled configuration. Review these commands to ensure that you have configured the device as desired.

- Run a Delta Configuration Summary to view the differences between the modeled configuration and the running configuration in CLI command format.

Update the device:

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

2. Select the devices or device groups you want to update and click OK. NetScreen-Security Manager begins updating the selected devices or device groups with the modeled configuration.

After updating:

- Review the information in the Job Information window to determine if the update was successful.

- NetScreen-Security Manager automatically runs a Delta Configuration Summary after a successful update. Review the summary to ensure that no conflict exist between the running configuration and the modeled configuration.

**Retrying a Failed Update**

When updating your managed security devices, the update fails for each device that is not connected to the management system at the time of update. For device running ScreenOS 5.1 or higher, you can configure NetScreen-Security Manager to save the pending changes for an unconnected device, then install those changes when the device finally connects to the management system.

NetScreen-Security Manager automatically changes the configuration state of an unconnected device that is waiting for changes to the “Sync Pending” state. When a device in this state connects to the management system, pending changes are immediately installed on the device and the configuration state is changed to “In-Sync”.

You can also configure the management system to abort update attempts for previously unconnected devices to which out-of-band changes have been made. For example, you attempt to update all your managed NS-5GT security devices, but device NS-5GT-25 is disconnected from the management system for troubleshooting at the time of update. When troubleshooting is complete and the device reconnects, to prevent NetScreen-Security Manager from overwriting any out-of-band changes made, enable the option “Don’t Update If Device Has Changed”.

**Configuring Update Options**

You can configure device update and retry options on a system-wide basis (in the UI preferences), on a per-update basis for multiple devices (in the device update dialog box), and on a per-update basis for a single device (in the device options dialog box). The system-wide settings appear as the default settings for the both per-update settings, which you can change as needed for each update.
When configuring system-wide update options, you can enable or disable any option independently; when configuring per-update options, dependencies apply.

Update options include:

- **Rematch, Session Treatment when modifying a policy rule**—When enabled, NetScreen-Security Manager preserves the existing sessions that are being tracked by the installed Security Policy during the policy update procedure (devices running ScreenOS 5.1 or higher only). At the end of the update, NetScreen-Security Manager restores all valid sessions on the managed device and deletes all invalid sessions.

  When disabled, NetScreen-Security Manager does not preserve and restore existing sessions for a updated managed device.

- **Show Unconnected Devices in Device Selection Dialog**—When enabled, the NetScreen-Security Manager UI displays devices that are not connected to the management system in the Update Devices dialog box (which displays when you attempt to update the configuration for a managed device).

  When disabled, unconnected devices do not appear in the Update Devices dialog box, preventing admins from selecting an unconnected device for updating.

  When configuring this option on a per-update basis, you must enable this option before the “Update When Device Connects” option is available.

- **Update When Device Connects**—When enabled, NetScreen-Security Manager attempts to update a previously unconnected device with pending changes stored in the management system.

  When disabled, NetScreen-Security Manager does not update a previously unconnected device, and the configuration state of the device remains as “Sync Pending”.

  When configuring this option on a per-update basis, you must enable this option before the “Don’t Update If Device Has Changed” option is available.

- **Don’t Update If Device Has Changed**—When enabled, NetScreen-Security Manager does not update a previously unconnected device if out-of-band changes have been made to the device. The configuration state of the device remains as “NSM and Device Changed”, or “Device Changed” when the update device job is cancelled due to a change on the device.

- **Enable Option Dialog**—When enabled, NetScreen-Security Manager displays device update options for single-device updates. The update options dialog box appears when you right-click a device in Device Manager and select Update Attacks.

  When disabled, the update options dialog box does not appear for single-device updates initiated from the Device Manager. Alternatively, to disable from within the per-update device update dialog box, select the option “Don’t Show This Dialog”.
Tracking Device Updates

Use Job Manager to track device updates in real-time. You can view the status of a running update and the status of completed updates in the Job Manager module.

When you send a command to a device or group of devices using NetScreen-Security Manager, the management system creates a job for that command and displays information about that job in the Job Information window. The command you send the device is called a directive; Job Manager tracks the progress of the directive as it travels to the device and back to the management system. Each job contains:

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

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

You can initiate directives from multiple locations in the NetScreen-Security Manager UI, including the Devices and Tools menus in the NetScreen-Security Manager toolbar (to access the Update directive, from the file menu, select Devices > Configuration > Update Device Configuration). The Job Manager module is shown below:
Figure 49: Job Manager Module

Job Manager includes the following utilities and information:

- **View Controls**—Use View controls to set the information level you want displayed in Job Manager:
  - Expand All displays all devices associated with a directive type.
  - Collapse All displays the directive type.

- **Job Type (Directive) List**—Displays the job type (directives) and associated time stamp completion status information. All current and completed jobs appear, including device updates. However, if you have not yet performed an update using NetScreen-Security Manager, the Job List does not display an Update Configuration directive.

- **Notification Controls**—Enables you to manually view job completion status.

- **Job Information**—Enables you to view various types of job information including errors, job completion status, job state, automatic job completion notification setting, and start time of job.
Reviewing Job Information

The Job Information dialog box displays the changing device states as the directive is executed. Device state changes, error messages, and warning messages are displayed in real-time. An example Job Information dialog box is shown below:

Figure 50: Job Information Dialog Box

Job Manager tracks the overall progress of one or more jobs executed on a single device. For multiple device updates, Job Manager tracks the progress of each job on each device in addition to the overall progress for all devices. To view the Job status for an individual device (including error messages and percent complete), select the device in the Percent Complete pane; the status appears in the Output pane.

The Job Information includes:

- **Job Type**—The type of task being tracked. Job Types include Update Device, Reboot Device, and Config Summary. Job Type is also known as a directive.
- **Time Stamp**—The time that NetScreen-Security Manager began executing the directive.
- **Job Status**—The current state of the job.
- **Number of Jobs Completed**—The number of jobs completed out of the total number of jobs.
- **Percent Complete**—The percentage of total jobs successfully executed. When performing multiple jobs on multiple devices, this number displays the percentage complete for each device. When the job has completed, successfully or unsuccessfully, the percent complete displays 100 percent.
- **Device Name**—The name of the device on which the job is executed.
- **State Description**—The current state of the job.
- **Completion Level**—The percentage of the total job that has executed successfully.

- **Output**—Displays content of the update, including commands that have been interpreted from the NetScreen-Security Manager data model into ScreenOS commands, error messages, and existing commands deleted from the device. The Output Display Region displays all errors, warnings, device verification output, and device state information associated with the job.

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

### Device States During Update

During an update, the managed device changes device state. You can view the current device state in real-time in the State Description field of the Job Information dialog box. A device can have the following states:

<table>
<thead>
<tr>
<th>Device State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>No update activity has occurred on the device.</td>
</tr>
<tr>
<td>Loading in Progress</td>
<td>NetScreen-Security Manager is sending the update image into the Flash memory of the device.</td>
</tr>
<tr>
<td>Pending</td>
<td>Device is accepting the parameters from the update configuration that has been sent to the device Flash memory.</td>
</tr>
<tr>
<td>Converting Data Model to Device Data Model</td>
<td>The parameters that have been set in the NetScreen-Security Manager configuration are being changed to corresponding ScreenOS CLI commands that execute on the device.</td>
</tr>
<tr>
<td>Completion</td>
<td>Device has successfully been updated with the modeled configuration.</td>
</tr>
<tr>
<td>Failed</td>
<td>Device has not been successfully updated with the modeled configuration. The Output pane of the Job Manager dialog box displays error messages and error codes.</td>
</tr>
</tbody>
</table>

The update process for devices running ScreenOS 4.0.x or ScreenOS 5.x is identical.

### Understanding Updating Errors

When an update fails for any reason, Job Manager displays error codes and error messages that can help you identify and locate the problem. Typical errors include:

- The modeled configuration contained invalid values that the device could not process.

- During the update process, the connection between the managed device and the Device Server was lost.
The modeled configuration caused the managed device to lose its connection to NetScreen-Security Manager. For these update errors, the Job Information dialog box displays the Job Status as “Failed.”

You can also check the Connection Status and Configuration Status columns for the device in the Realtime Monitor to determine if the device is running.

After a device is updated, NetScreen-Security Manager automatically runs a Delta Configuration Summary to determine any remaining differences between the modeled configuration and the running configuration; the output of this summary appears in the Job Manager information window. For successful updates, no discrepancies are found or displayed. For failed updates, the output area lists remaining discrepancies.

For example, a failed update job is shown below:

Figure 51: Failed Update Job Dialog Box

In the Output area of this job, the update:

- Successfully removed existing commands on the device (Generating Removing CLI Commands)
- Unsuccessfully added new commands that were not present in the running configuration (Generated 5 Delta Config CLI Commands). Specifically, the update could not set the command: pppoe name untrust clear-on-disconnect

The Delta Config Summary correctly detected a difference between settings on the managed device and settings in NetScreen-Security Manager. This error might be the result of a disabled command, possibly disabled by another NetScreen-Security Manager administrator or a local device administrator.
Chapter 7
Managing Devices

This chapter describes device management tasks you might need to perform in specific situations, such as upgrading the ScreenOS version on your devices, obtaining and activating a Deep Inspection subscription, and handling an RMA device in the NetScreen-Security Manager UI.

This chapter also provides details on how the components of the NetScreen-Security Manager management system handle device capabilities, and how device configuration settings are imported and updated. This material is provided for reference only, and does not contain specific configuration tasks.

This chapter contains the following sections:

- Managing Device Firmware Version on page 194
- Managing License Keys on page 196
- Activating Subscription Services on page 197
- Managing the Attack Database on page 197
- Updating AV Pattern Files on page 208
- Updating the Web Category List on page 209
- Miscellaneous Device Operations on page 209
- Managing Device Capabilities on page 214
- Archiving and Restoring on page 219
Managing Device Firmware Version

You can use Juniper Networks NetScreen-Security Manager to upgrade or adjust the firmware on a device running ScreenOS 4.0.x or higher, or IDP 4.1 or higher.

NOTE: NetScreen-Security Manager does not support the upgrade of NetScreen-500 and ISG 2000 security devices from ScreenOS 5.1 to ScreenOS 5.2. This migration requires a bootrom upgrade; for more details, refer to the ScreenOS 5.2 Migration Guide.

Upgrading Device Firmware Version

To upgrade the firmware, first download the new firmware image file to your computer. Next, use the Firmware Manager (Tools > Firmware Manager) in NetScreen-Security Manager to copy the image file to the GUI Server, where it is permanently stored, then select the devices and the firmware images you want to use to upgrade the device. During the upgrade (Devices > Firmware > Change Device Firmware), the GUI Server copies the image file to the Device Server, where the image file is stored temporarily until the upgrade is complete. After the firmware has been successfully installed, the device automatically reboots.

NOTE: Do not change the name of the image file. The name of the image file must be exactly the same as the filename that you download from Juniper Networks, for example, ns5xp.4.0.3r2.0 or sensor_4_1r1.sh.

When upgrading multiple device types, ensure 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 device type must exist on the Device Server and must be the same OS version.

When upgrading firmware on your managed devices, you can use different methods depending on the OS version that exists on the devices:

- For devices currently running ScreenOS 4.0.x, you must install a TFTP server on the NetScreen-Security Manager Device Server. The Device Server automatically uses TFTP to load the firmware onto your managed devices. For more information, see the NetScreen-Security Manager Installer's Guide.

- For devices running ScreenOS 5.x, the Device Server automatically uses Secure Server Protocol (SSP) to load firmware onto your managed devices. SSP is the protocol used for the management connection between the physical device and the NetScreen-Security Manager Device Server.

- For devices running IDP Sensor software, the Device Server uses SSH/SFTP to upload and run the upgrade software. The Management Port on the IDP Sensor must be active and reachable over the network via SSH.
Select the Automate ADM Transformation option to automatically update the Abstract Data Model (ADM) when the firmware is loaded onto the managed device. If you deselect this option, the firmware is loaded onto the device, but you cannot manage the device from the UI until the ADM is updated. For example, you might want to deselect this option to first verify that the device is properly operating with the uploaded firmware before managing it from the NetScreen-Security Manager UI. To enable management, you must reconcile the firmware that you uploaded on the device with the ADM, as described in “Adjusting Device Firmware Version” on page 195. For more information about the ADM and NetScreen-Security Manager components, see “Managing Device Capabilities” on page 214.

For step-by-step instructions on upgrading a device, see the NetScreen-Security Manager Online Help topic, “Upgrading Firmware on Devices.”

Adjusting Device Firmware Version

When importing or updating devices, NetScreen-Security Manager alerts you if it detects a mismatch between the firmware running on the managed device and the firmware that NetScreen-Security Manager has recorded for the device.

Firmware mismatches can occur when:

- A device administrator changes the firmware on the device using the WebUI or CLI commands (through a console, Telnet, or SSH session).
- The Automate ADM Transformation option in the Firmware Update Availability dialog box was deselected during a firmware upgrade by NetScreen-Security Manager. (See “Upgrading Device Firmware Version” on page 194.)

To reconcile the firmware versions, right-click a device and select Adjust OS Version to display the Adjust OS Version Wizard. Follow the directions in the wizard. For step-by-step instructions on upgrade a device, see the NetScreen-Security Manager Online Help topic, “Adjusting the Firmware Version on Devices.”

Downgrading Device Firmware Version

NetScreen-Security Manager does not support firmware downgrades; you cannot use NetScreen-Security Manager to install an earlier version of Juniper Networks ScreenOS firmware than is currently running on the device. You must use the WebUI or ScreenOS CLI commands to downgrade a managed device, then re-add the device to NetScreen-Security Manager.

Upgrading Device Support

Use the Upgrade Device Support directive to automatically upgrade all existing devices that are eligible to provide forward or full management support for features in a future release of ScreenOS.

NOTE: You must install a schema patch for the future version of ScreenOS before upgrading the device support.

The directive performs the following actions:
Performing an Adjust OS Version from the previously-known ScreenOS version to the new version of ScreenOS running on the selected devices.

- Optionally performs an import on the selected devices.

Managing License Keys

Some security devices support the activation of optional features or the increased capacity of existing features through the installation of license keys. You must first obtain a license key from your value-added reseller (VAR) or from Juniper Networks, then you can use the NetScreen-Security Manager UI to install the license key on the managed device.

After you have installed the license key on the device, the device can begin to use the new feature immediately. However, because the information in the license key is decoded only after it has been installed on the device, you must import the license key information from the device into the NetScreen-Security Manager system before the new feature displays in the UI. Importing license keys from the device can also resolve any license key mismatches between NetScreen-Security Manager and the managed device.

Installing License Keys

The procedure for obtaining a license key is as follows:

1. Contact the value-added reseller (VAR) who sold you the security device, or contact Juniper Networks directly.

2. Provide the serial number of your device and state the feature option you want. The license key is generated and then sent to you via email.

To install the license key on a device using the NetScreen-Security Manager UI:

1. In the main navigation tree, right-click the device on which you want to install the licence key and select Admin > Install License Key. The Install License Key dialog box appears.

2. Either copy and paste the license key into the dialog box, or click the Browse button to locate the license key file on your computer.

3. Click OK.

Importing License Key Information

After you install a new license key on a device, either through the NetScreen-Security Manager UI or locally (through the WebUI or CLI) you must import that license key information into the NetScreen-Security Manager system.

Importing license key information from a device also enables you to quickly view all license keys installed on a device, and the features and capacities available on the device.

To import or view license key information:
1. In the main navigation tree, right-click the device on which you want to install the licence key and select Admin > Get License Key Info.

2. Click Yes at the confirmation dialog box. The Job Information window displays the license key information.

Installing Trial License Keys

For devices running ScreenOS 5.3 and above, you can install a trial license key. A trial license key allows you to view and evaluate specific features on the device before purchasing the subscription.

Activating Subscription Services

To use some Juniper Networks services, such as internal AV or Deep Inspection Signature Service, you must activate the service on the device by first registering the device, then obtaining the subscription for the service. Even though devices with bundled AV services come with a temporary, pre-installed subscription, you must register your product and retrieve the subscription to receive your full paid subscription.

To register your product, go to www.juniper.net/support. After you have registered your product, you can retrieve the service subscription as described in the following section.

To obtain the subscription for a service:

1. From the menu bar, select Devices > Entitlement > Get Entitlement. The Get Entitlement dialog box appears.

2. Select the device(s) or group of devices for which you want to retrieve a subscription.

3. Click OK. The Job Information window displays the status of the subscription retrieval.

Managing the Attack Database

The attack object database stored on the device contains predefined attack objects and groups designed to detect known attack patterns and protocol anomalies within network traffic. You use attack object when using Deep Inspection (DI) or Intrusion Detection and Prevention (IDP) as attack detection mechanisms in a Security Policy rule.

To manage the attack database:

- Updating the Attack Object Database—Juniper Networks provides frequent attack database updates, available for download from the Juniper Networks website. New attacks are discovered daily, so it's important to keep your attack object database up-to-date.

- Verifying the Attack Database Version—The attack database version on the security device and on the NetScreen-Security Manager GUI Server must match.
- Updating the IDP Detector Engine—The IDP engine is dynamically changeable firmware that runs on IDP Sensors and on the optional Security Modules for the ISG family of devices.

- Scheduling Security Updates—Configure the NetScreen-Security Manager system to automatically update your security devices with the latest attack objects.

The following sections detail each activity.

### Updating the Attack Object Database

You can update the attack object database for managed devices that have Deep Inspection or IDP capabilities.

- For devices running ScreenOS version 5.0.0-IDP1, ScreenOS 5.1 and higher, or standalone IDP, you must download new attack objects from the attack object database server to the GUI Server, then download the new objects to your managed devices. IDP attack objects are loaded automatically when an IDP rulebase is loaded; DI attack objects must be loaded manually.

- For devices running ScreenOS versions 5.0 or earlier, you must configure the devices to contact the attack object database server, then prompt the devices to download new attack objects from the server.

To update a managed device with new DI attack objects, you must first obtain a DI subscription for your security device. For details, see “Activating Subscription Services” on page 197.

### Updating Attacks for IDP-enabled devices

You can update attacks by downloading new attack objects and a new detector engine from the attack object database server to the GUI Server, then downloading the new objects to your managed devices.

You can perform a network update if the NetScreen-Security Manager GUI Server has an Internet connection, either directly or through a proxy. During a network update, the GUI Server contacts the Attack Object Database server (managed by Juniper Networks) and automatically downloads the necessary attack object files.

You can perform a local update if the GUI Server does not have Internet connectivity or you do not want to perform a network update. To prepare for a local update, you manually download the attack objects files from the Attack Object Database server (managed by Juniper Networks), then copy these files to a local directory on the GUI Server. Then, during the local update, you specify the path to these files.

### Preparing for a Local Update

To perform a local update, you must complete the following steps before attempting the update:

1. Obtain the attack update data file from Juniper Networks website.
Chapter 7: Managing Devices

Managing the Attack Database


Copy and paste the content from the URL into a text file called NSM-SecurityUpdateInfo.dat.

Make sure the file has no HTML tags, RTF tags, or control characters. Use a text editor to make sure there are no control characters in the file. The file should begin with

```
(updateInfo
```

and end with a closing paren

```
)
```

2. Open the .dat file and locate the “url” line. For example:

```
:url ("NSMFP6-DI-IDP.zip")
```

The zip filename is the name of the attack database zip file.

3. Download the attack database zip file from https://services.netscreen.com/restricted/sigupdates/nsm-updates/<zipFileName>.

   For example:
   https://services.netscreen.com/restricted/sigupdates/nsm-updates/NSMFP6-DI-IDP.zip

Download the file to your local disk. Do not change the filename.

4. Put both files in a local directory on the NetScreen-Security Manager GUI Server or on an internal web server that is reachable by the NSM GUI Server.

5. Change the permissions on both files to make them readable by all users, but do not change the filenames.

Running the Attack Object Update (Local and Network)
To update the attack object database on the NetScreen-Security Manager GUI Server:

1. Navigate to the global domain.

   You can only update the attack object update settings and download a new attack object database from the global domain.

2. Select Tools > Preferences to open the New Preferences dialog box.

3. In the preference navigation tree, select Attack Object.

4. In the Download URL box, configure the URL for the attack update file. When you update the attack object database, the management system contacts this server and downloads the latest database version to the GUI Server.
To perform a network update, enter the URL of the Attack Object Database web server in the Download URL box. To restore the default server, select Restore Defaults.

To perform a local update, specify the local directory path to the .dat file you previously downloaded in the Download URL box. Example: file:// / / tmp/NSM-SecurityUpdateInfo.dat

To use a proxy server for attack object download, select the Enable Proxy checkbox. Then, enter the proxy server IP address, port, user name, and password.

For DI devices, click the + button to enter a DI license key and specify Deep Inspection Packs.

5. Select Tools > Update NSM Attack Database. The Update NSM Attack Database dialog box appears.

6. Follow the instructions in the Attack Update Manager to download the new Signature and Protocol Anomaly Attack Objects to the NetScreen-Security Manager GUI Server.

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

IDP attack objects are loaded automatically when you load an IDP rulebase. DI attack objects must be loaded manually.

To load the DI attack object database update to your managed devices:

1. Select Devices > Deep Inspection > Update Device Attack Database. The Update Device Attack Database dialog box appears.

2. Click Next, then select the managed devices on which you want to install the attack object update.

3. Follow the directions in the Change Device Sigpack wizard to update the attack object database on the selected managed devices.

Updating DI Attacks on ScreenOS 5.0 and Lower Devices

You can update attacks for ScreenOS 5.0 and lower devices (not 5.0.0 IDP1) by configuring your managed devices to contact the attack object database server, then prompting the devices to download new attack objects from the server.

To configure the device to contact the attack object database server:

1. In the main navigation tree, select Device Manager > Security Devices, then double-click the device for which you want to configure the database.

2. In the device navigation tree, select Security > AttackDB > Settings.

3. For Attack Database Server, enter https://services.netscreen.com/restricted/sigupdates
4. For Mode, select **Update**.

5. Click **OK** to save your changes.

For details, see “NetScreen-Security Manager: Configuring Firewall/VPN Devices”.

To prompt your managed devices to contact the server for updates:

1. From the menu bar, select **Devices > Deep Inspection > Update Device Attack Database**. The Update Device Attack Database dialog box appears.

2. Click **Next**, then select the managed devices that you want to update their attack object database.

3. Follow the directions in the Change Device Sigpack wizard.

**Using Updated Attack Objects**

After you download updated attack objects and groups to the GUI Server (or to the device), any new attack objects in the update are available for selection in NetScreen-Security Manager Object Manager. Additionally, updated IDP attack objects also appear available for selection within an IDP rulebase in a Security Policy.

You can use new and updated DI attack objects immediately within a DI profile (in a firewall rule), or use the new and updated IDP attack object within an IDP rulebase.

When you install the Security Policy on your managed security devices:

- For a Security Policy that uses IDP attack objects, NetScreen-Security Manager pushes only the attack objects that are used in IDP rules for the device from the GUI Server to the device.

- For a Security Policy that uses DI attack objects, NetScreen-Security Manager pushes all updated signatures from the GUI Server to the device.

**Verifying the Attack Database Version**

New attack objects are added to the attack object database server frequently; downloading these updates and installing them on your managed devices regularly ensures that your network is effectively protected against the latest threats. As new attack objects are added to the attack object database server, the version number of the database increments by 1. When you download a version of the attack object database from the server, NetScreen-Security Manager stores the version number of that database.

**Automatic Verification**

The management system uses the database version number to detect and notify you when the stored attack object database on the GUI server is:

- Older than the most recent database available from the attack object database server, and/or

- Newer than the attack object database currently installed on your ScreenOS 5.1 and higher managed devices.
When NetScreen-Security Manager detects that managed device contains an older attack object database version than the one stored on the GUI Server, the UI automatically displays a warning for that device indicating that you should update the attack object database on the device.

Manual Verification

You can also manually check to see if the attack object database on the server is more recent than the one on the security device.

To manually check the attack object database version:

2. Select the device(s) or group of devices to be checked.
3. Click OK. The Job Information window displays the status of the version check.

Managing Different Attack Database Versions

Each managed device can contain a different attack object database version, however, the NetScreen-Security Manager GUI Server can contain only one version of the attack object database at one time. Therefore, when you update the device configuration on a device, you must also update the database on the managed device to match the version of the database on the GUI Server (if the version on the GUI Server is more recent). If the version on the managed device is identical to or more recent than the version on the GUI Server, the device ignores the attack object updates.

Although devices running 4.0.x or 5.0 update their attack object database independently of the GUI Server, they also must remain in sync with the attack object database version on the management system if you intend to disable attacks at the device level:

- When the databases are in sync, you can disable attacks at the device level.
- When the databases are out of sync, you cannot disable attacks at the device level. You must update the attack object database on the device using the procedure detailed in “Updating DI Attacks on ScreenOS 5.0 and Lower Devices” on page 200.

For details on disabling attacks, see “NetScreen-Security Manager: Configuring Firewall/VPN Devices”.

NOTE: Although each managed device can contain a different attack object database version, we recommend that you use the most recent version of the attack object database available to ensure that your network is protected against the latest threats.
EXAMPLE: UPDATING DEVICES WITH DIFFERENT ATTACK OBJECT DATABASE VERSIONS

On Monday, you update the attack object database to version 2.0 on the GUI Server, then update two managed devices running ScreenOS 5.2, Device A and Device B. Both devices (and the GUI Server) have the same version of the attack object database.

On Wednesday, in response to a security alert, you update the attack object database to version 2.1 on the GUI server, but install the update on only one of your managed devices, Device A. Device A (and the GUI Server) is now running a different version of the attack object database than Device B.

On Friday, you make miscellaneous configuration changes to Device A and B, then attempt to update both devices with the modeled configuration. During the update, the UI warns you that Device B is running an older version of the attack object database than the GUI Server contains.

Updating the IDP Detector Engine

The IDP engine is dynamically changeable firmware that runs on ISG security devices running ScreenOS 5.0.0-IDP1 and on standalone IDP Sensors. Automatic updates to the IDP engine occur when you:

- Upgrade security device Firmware—When you upgrade the firmware, the upgraded firmware includes the most recent version of the IDP engine as well as a new version of ScreenOS.
- Manually load a new detector engine—New detector engines may be downloaded with normal attack object updates. But, the new detector engine must be load onto the device separately. Use Devices > IDP Detector Engine > Load IDP Detector Engine to load the new detector onto devices.

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

To update the IDP Engine manually:

1. From the menu bar, select Devices > IDP Detector Engine > IDP Detector Engine. The Change Device Sigpack dialog box appears.
2. Click Next, then select the managed devices on which you want to install the IDP engine update.
3. Follow the instructions in the Change Device Manager to update the IDP engine on the selected device.

NOTE: Updating the IDP engine on a device does not require a reboot of the device.

You can also download the new detector engine automatically. See Scheduling Security Updates on page 204.
EXAMPLE: CONFIRM IDP ENGINE VERSION
To see the version of the IDP engine that is currently running on a ISG 2000 or ISG 1000 device:


2. Click Next. The Attack Update Summary displays information about the current version downloaded on the GUI Server and the latest version available from Juniper Networks.

Figure 52: Attack Update Summary

3. Click Cancel to exit the Attack Update Manager.

Scheduling Security Updates
For security devices running ScreenOS 5.0.0-IDP1, 5.1 or higher and IDP 4.0 and higher, you can configure the NetScreen-Security Manager system to automatically update the attack object database on the GUI Server and on those security devices.
For ScreenOS devices running ScreenOS 5.0.x and lower (except for ScreenOS 5.0.0-IDP1), NetScreen-Security Manager does not automatically install new attack objects on the device but instead flags the device for manual updating using the UI.

**NOTE:** Unlike the GUI-based attack object updates, Scheduled Security Updates automatically pushes any new IDP detector engine that has been downloaded.

Using the command line utility `/usr/netscreen/GuiSvr/utils/guiSvrCli.sh`, direct the management system to obtain the latest attack objects from the attack database server (managed by Juniper Networks), then specify the action you want the server to take.

For a successful update, the device configuration must be “In-Sync”, meaning that the device is connected and that no configuration differences exist between the configuration on the physical device and the modeled configuration in NetScreen-Security Manager, or “Sync Pending”, meaning that the device is unconnected and that the physical device will be updated with the modeled configuration when the device reconnects to the management system. However, if a device is connected but its configuration is not “In-Sync”, the update process skips that device to avoid installing unexpected changes.

To handle unconnected devices during the update, you must also specify additional post-action options.

Table 18: Scheduled Security Update (SSU) Command Line Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>--help</td>
<td>Lists command line options for guiSvrCli.sh.</td>
</tr>
<tr>
<td>--update-attacks</td>
<td>This command directs the system to update its attack database by connecting to and downloading the latest attack database, if newer. Requires post-action parameter.</td>
</tr>
<tr>
<td>--post-action</td>
<td>Indicates that a post action instruction will follow (none or update-devices). Requires none or update-devices parameter.</td>
</tr>
<tr>
<td>--none</td>
<td>No post action. SSU updates the attack database, but does not push the new attacks to devices. No other parameters needed.</td>
</tr>
<tr>
<td>--update-devices</td>
<td>Updated managed security devices with newly updated attack objects. The device must be connected to the management system with an “In-Sync” configuration status OR unconnected with a “Sync Pending” configuration status. If a device is connected but its configuration is not “In-Sync”, the update process skips that device to avoid installing unexpected changes. Requires an unconnected devices handling option (skip or retry).</td>
</tr>
</tbody>
</table>
Table 18: Scheduled Security Update (SSU) Command Line Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--skip</td>
<td>Directs the server to skip any unconnected device (server does not try to update attack objects on that device.) No other parameters needed.</td>
</tr>
<tr>
<td>--retry</td>
<td>Directs the server to update the device the next time it connects. If the device has changed while offline, the server will take action based on the next parameter. Requires modified device parameter (abort or override).</td>
</tr>
<tr>
<td>--abort</td>
<td>Directs the server to abort the update attempt if the device has changed while offline. The device configuration state is set to “Both Changed”, indication that both the device and NetScreen-Security Manager have pending changes.</td>
</tr>
<tr>
<td>--override</td>
<td>Directs the server to update the device with the new attack objects, overwriting any out-of-band changes made to the device.</td>
</tr>
</tbody>
</table>

EXAMPLE: UPDATE ATTACK OBJECTS AND PUSH TO CONNECTED DEVICES
To download a new attack database and push it to connected devices only (ignore unconnected devices), use the following command line.

```bash
/usr/netscreen/GuiSvr/utils/guiSvrCli.sh --update-attacks --post-action
--update-devices --skip
```

Scheduling the Update
You can perform a one-time security update using guiSvrCli.sh directly, or you can use crontab (or other scheduling utility) to configure the update to run at the intervals you desire.

NOTE: Before performing or scheduling a security update, Juniper Networks recommends that you disable the auto-update setting for all managed devices. To disable this setting in the device configuration, from the device navigation tree, select Security > Attack DB > Settings, then set the Schedule Mode to Disable.

To perform a one-time security update:

1. Log in to the NetScreen-Security Manager GUI Server as root.
2. Change to the utility directory by typing: cd /usr/netscreen/GuiSvr/utils.
3. Type the following to update attacks, including specifying the post action options for the update:

   ```bash
   guiSvrCli.sh --update-attacks --post-action <post-action options>
   ```

4. Enter your domain/username and password when prompted.

To configure a scheduled security update using cron tab:
1. Log into the GUI server.

2. Change to the utility directory by typing: `cd /usr/netscreen/GuiSvr/utils`.

3. Create a shell script with the following elements:
   - Set the NSMUSER environment variable with an NSM domain/user pair. The command for setting environment variables depends on your OS.
     
     Example: `export NSMUSER=domain/user`
   
   - Set the NSMPASSWD environment variable with an NSM password. The command for setting environment variables depends on your OS and shell.
     
     Example: `export NSMPASSWD=password`
   
   - Specify a guiSvrCli command string.
     
     Example: `/usr/netscreen/GuiSvr/utils/guiSvrCli.sh --update-attacks --post-action post_action_options`

4. Make the script executable. Make sure the script is runnable by whoever will create the cron job.

5. Run the crontab editor.
   
   `crontab -e`

6. Add an entry for the shell script
   
   `<minutes after hour> <hour> * * * path/attack_update_shell_script`

During the update, the guiSvrCli utility updates its the attack object database, then performs the post actions. After updating and executing actions, the system generates an exit status code of 0 (no errors) or 1 (errors).

**EXAMPLE: USING CRON TAB TO SCHEDULE ATTACK UPDATES**

In this example, you want to use cron tab to update attack objects for online managed security devices every day at 5:00am. This example assumes you are running on Linux, that you have a domain called `idp`, and that there is an NSM user called `idpadmin`.

1. Log into the GUI server.

2. Change to the utility directory by typing: `cd /usr/netscreen/GuiSvr/utils`.

3. Create a shell script called `attackupdates.sh` with the following contents.
   
   ```bash
   export NSMUSER=idp/idpadmin
   export NSMPASSWD=idpadminpassword
   /usr/netscreen/GuiSvr/utils/guiSvrCli.sh --update-attacks --post-action
   --update-devices --skip
   ```

4. Make the script executable.
chmod 700 attackupdates.sh

5. Run the crontab editor.

crontab -e

6. Add the script to the crontab.

```
0 5 * * * /usr/netscreen/GuiSvr/utils/attackupdates.sh
```

You can view expanded update results using the Job Manager and Audit Log Viewer in the NetScreen-Security Manager UI, as detailed in the following sections.

**Viewing Scheduled Security Updates in the Job Manager**

Each scheduled security update generates a Job Manager entry, entitled Scheduled Attack and Device Update. The entry contains job status information, such as “connected to server” or “no new security update available”.

If the post-action was update-attacks, the job information also includes:

- A list of devices that the server attempted to update with new attack objects.
- For each device, the status of the update, such as “update successful”, “device skipped due to pending changes”, or “update aborted”.

To view a Job Manager entry, in the main navigation tree of the NetScreen-Security Manager UI, select Job Manager then doubleclick the entry you want to view.

**Viewing Scheduled Security Updates in the Audit Log Viewer**

Each scheduled security update generates an entry in the Audit Log Viewer. The entry contains the following information:

- Time Generated—Specifies the time at which the update began.
- Admin Name/Domain—The admin name for security update is guiSvrCli and the domain is Global (entry appears as guiSvrCli/Global).
- Action—The action appears as “Scheduled Attack and Device Update”.

To view an audit log entry, in the main navigation tree of the NetScreen-Security Manager UI, select Audit Log Viewer.

### Updating AV Pattern Files

Some security devices provide antivirus (AV) scanning for specific application-layer transactions using an internal AV scanner developed by Trend Micro. The internal AV scanner references a virus pattern file to identify virus signatures. As new viruses emerge, the pattern file on the device needs to be updated.

To update the AV pattern file for a device:
1. From the menu bar, select **Devices > AV Scan Manager > Update Pattern**. The Update Pattern dialog box appears.

2. Select the device(s) or group of devices to be updated.

3. Click **OK**. The Job Information window displays the status of the update.

### Updating the Web Category List

Web categories (predefined by SurfControl) are used to create the default WEB Filtering Profile object, which you can use in a firewall rule to permit or deny specific URL requests to or from your protected network.

The SurfControl CPA server periodically updates its predefined category list, but does not notify its clients when the list is updated. To ensure that the security device and NetScreen-Security Manager use most up-to-date predefined categories, you must update the list manually, first on the device, then for the NetScreen-Security Manager system.

---

**NOTE:** The security device periodically polls the CPA server for category updates. The default interval is every two weeks; for details on changing this settings, see “NetScreen-Security Manager: Configuring Firewall/VPN Devices”.

You must perform both steps listed below, in the following order:

1. In the menu bar, select **Devices > WEB Filtering > Update Web Categories**. This option updates the security device predefined categories from the SurfControl CPA server.

   You must perform this step before updating the categories on the NetScreen-Security Manager management system. When the Select Devices dialog box appears, select the security device you want to contact SurfControl.

2. In the menu bar, select **Devices > WEB Filtering > Update System Categories**. This option updates the NetScreen-Security Manager management system predefined categories from a security device.

   You must perform this step after updating the predefined categories on the security device.

### Miscellaneous Device Operations

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

- Restarting Devices
- Refreshing DNS Entries
- Updating the Device Clock with an NTP Server
- Setting the Root Administrator on a Device
The following sections detail each management task.

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

1. From the menu bar, select Devices > Reboot Device. The Reboot Device(s) dialog box appears.
2. Select the device(s) or the group of devices to be restarted.
3. Click OK. The Job Information window displays the status of the restart.

Refreshing DNS Entries
To enable a security device to use Domain Name System (DNS) to resolve domain names to IP addresses, you configure the IP addresses of the primary and secondary DNS servers on the device. The device can automatically refresh entries in its DNS table by checking them with the specified DNS server at regularly scheduled times or intervals, or after an HA failover).

You can also manually direct the device to refresh its DNS table entries. When you direct the device to refresh its DNS entries, it connects to the previously-configured DNS server to perform a lookup of each entry in its table.

To direct one or more devices to refresh their DNS table entries:

1. Select DNS > Refresh DNS Entries from the Devices menu. The Refresh DNS Entries dialog box appears.
2. Select the device(s) or the group of devices on which DNS tables should be refreshed.
3. Click OK. The Job Information window displays the status of the refresh.
**Updating the Device Clock with an NTP Server**

The security device can use the Network Time Protocol (NTP) to synchronize its system clock with a configured NTP server over the Internet. You can configure the device to perform this synchronization automatically at specific time intervals (see “NetScreen-Security Manager: Configuring Firewall/VPN 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. From the menu bar, select Devices > NTP > Perform NTP Time Update. The Perform NTP Time Update dialog box appears.
2. Select the device(s) or group of devices that should be synchronized with NTP servers.
3. Click OK. The Job Information window displays the status of the synchronization.

**Setting the Root Administrator on a Device**

All security devices ship with the same default login and password for the root administrator. Because these default settings are known, you should change the login and password for the root administrator as soon as possible and as often as necessary.

Each security device can have only one root administrator, who has the following privileges:

- Manages the root system of the security device
- Adds, removes, and manages all other administrators
- Establishes and manages virtual systems, and assigns physical or logical interfaces to them
- Creates, removes, and manages virtual routers
- Adds, removes, and manages security zones
- Assigns interfaces to security zones
- Performs asset recovery
- Sets the device to FIPS mode
- Resets the device to its default settings
- Updates the firmware
- Loads configuration files

**NOTE:** All passwords handled by NetScreen-Security Manager are case-sensitive.
After you change the root administrator login and password, only persons who know the new login and password can log into the device and perform the tasks listed above.

To configure the login and password for the root administrator for a security device:

1. In Device Manager, right-click a device icon select Admin > Set Root Admin. The Set Root Admin dialog box appears for the device.
2. Enter the new name in the Administrator Name field.
3. Enter the new password in the Password field and then re-enter the same password in the Confirm Password field.
4. Click OK.

For more details on managing device administrators, including the root administrator, see “NetScreen-Security Manager: Configuring Firewall/VPN Devices”.

**Failing Over/Reverting Back Interfaces**

Some security devices support port modes that bind a second backup interface to the Untrust zone. For these port modes, the backup interface is used only when there is a failure on the connection through the primary interface or when you manually force traffic from the primary interface to the backup.

To force a security device to fail over to the backup interface:

1. Right-click a device from the security device Tree or the security device List tab in the Device Manager and select Admin > Failover. The Failover Action dialog box appears.
2. Click Force to Failover.
3. Click OK.

To force a security device to revert back to the primary interface:

1. Right-click a device from the security device Tree or the security device List tab in the Device Manager and select Admin > Failover. The Failover Action dialog box appears.
2. Click Force to Revert.
3. Click OK.
Setting RMA State on a Device

If you need to send a device back to the factory and replace it with a new device, you can set the device to the RMA state. This state allows NetScreen-Security Manager to retain the device configuration without a serial number or connection statistics. When you install the replacement device, all you need to do is activate the device with the serial number of the replacement unit.

**NOTE:** The replacement device must be the same platform and ScreenOS version as the unit that is being replaced. Setting the RMA state cannot be undone.

In the RMA state, the device object is functionally identical to a modeled device, but its status is “RMA” in the Device Monitor.

To set a device to the RMA state:

1. Right-click a device from the security device Tree or security device List tab in the Device Manager and select RMA Device. The Confirm RMA Device dialog box appears.
2. Click OK. In the Device Monitor window, the device status is RMA.

When the replacement device is installed, activate the device with the serial number of the replacement. For information about activating a device, see “Activating a Device” on page 106.

**NOTE:** If you are placing an HA device in the RMA state, it is highly recommended that you perform a flash sync immediately after activating and updating that device. This will ensure that the configuration from the non-RMAed device to the RMAed device is synchronized. The flash sync ensures that the two HA devices are in sync in NSRP. It also ensures that the case sensitivity of the original zone name is preserved on the RMAed device.

Troubleshooting a BGP Peer Session on a Device

To troubleshoot BGP peer configurations, you can connect and disconnect BGP connections to a specific neighbor. You can also test the TCP connection to a specific neighbor. To perform these tests, you need to have configured a virtual router and the BGP dynamic routing protocol on the device, and enabled BGP on the virtual router and on the interface to the BGP neighbor.

To connect or disconnect to a BGP peer:

1. In the main navigation tree, select Device Manager > Security Devices. Right-click a device and select Admin > Modify BGP Peer Session. The Modify BGP Peer Session dialog box appears.
2. Select the virtual router in which the BGP configuration resides.
3. Select the peer to which you want to connect or disconnect from the list of configured BGP neighbors.
4. Select Connect to establish a BGP connection to the selected peer, Disconnect to terminate the BGP connection to the selected peer, or TCP Connect to test the TCP connection to the selected peer.

5. Click OK.

**Displaying CLI Commands on a Device**

| NOTE: | This task is only applicable to added security devices running ScreenOS 4.x with dynamic IP addresses. |

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

**Reactivating Wireless Connections**

You can deploy a Juniper Networks NetScreen-5GT Wireless security device running ScreenOS 5.0.0-WLAN as a wireless access point (WAP). When you make changes to the wireless settings for the security device, you must update the device with your changes before the new settings take effect. Additionally, the device must reactivate its WLAN subsystem to use the new settings. **NetScreen-Security Manager automatically reacts the WLAN subsystem within the wireless security device during the device update process.**

| NOTE: | When using an authentication server for wireless authentication, if you enable 802.1X support on that server, you must also reactive the WLAN subsystem before the change can take effect. |

The reactivation process takes several seconds (approximately 10 seconds) to complete. During reactivation of the WLAN subsystem, the device severs all wireless connections and clears all wireless sessions from the session table. Previously connected wireless clients must reconnect to reestablish their disrupted sessions.

For details on configure wireless settings, see “NetScreen-Security Manager: Configuring Firewall/VPN Devices“.

**Finding Usages**

To locate groups, vsys, policies, and VPNs that reference a specific device, right-click a device select Find Usages. The Find References box appears.

**Managing Device Capabilities**

This section presents a detailed description of how NetScreen-Security Manager components enable you to add, configure, update, and manage security devices. The illustration below is an overview of the components and how they interact with each other. A description of each component follows.
Abstract Data Model

The Abstract Data Model (ADM) is an XML file that contains configuration data for all objects in a specific domain. The ADM is stored in the GUI Server, but you do not access the ADM directly. When you create, update, or import a device, the GUI Server edits the ADM to reflect the changes. The Management console uses the ADM to determine the current options, fields, screens, and data range to display in the UI for each object.

Data Model

A Data Model (DM) is an XML file that contains configuration data for an individual device. The DM is stored in the Device Server. When you create, update, or import a device, the GUI Server edits the ADM to reflect the changes, then translates that information to the DM.
Data Model Schema

The structure of the ADM and DM is determined by the Data Model (DM) schema. The DM schema reads from a device capability file to determine the supported features for the ScreenOS version that is running on the managed devices. A device capability file lists the fields and attributes that a specific ScreenOS version supports.

Your network may contain similar security devices that are running different ScreenOS versions. For example, a NetScreen-5XT may run ScreenOS 5.x, which supports the Routing Information Protocol (RIP), while another NetScreen-5XT runs ScreenOS 4.0.0r2, which does not support RIP. The DM schema links to the appropriate device capability file for each device.

Device capability files make it easier to integrate devices into NetScreen-Security Manager and also make upgrading the software on your security devices easier. Each software release includes device capability files that describe the new and changed fields, attributes, and allowable ranges of values.

Data Model Updating

Data Model update is the process of translating the objects and object attributes in the ADM domain into individual DMs with device-specific configuration information.

In the ADM, objects are arranged similarly to objects in the management console: each item (VPN, policy, device, device group, and so on) is represented by an object. In the DM, each item is a property of a single device. During the data model update process, the GUI Server identifies the objects that contain properties for a device, and translates those object properties into properties of that device.

When you update a device configuration using the management console, the GUI Server translates the objects and object attributes in the ADM domain into device configuration information in a DM. The Device Server then translates the device configuration information in the DM into CLI commands and sends the commands to the device.
For example, the ADM contains a VPN with tunnel interfaces, a routing table, and users. When you update a selected device, the DM update identifies the devices that are involved in the VPN and creates interfaces, routing tables, users, and VPN rules in the DM for each device. The DM contains only the VPN information that relates to the specific device, not the entire VPN.

During the device model update process:

- The GUI Server translates the object and object attributes in the ADM domain into device configuration information in a DM.

- The Device Server translates the device configuration information in the DM into CLI commands.

- The Device Server sends the CLI commands to the device.
Data Model Importing

Data Model Import (DM import) is the process of translating the device-specific configuration information in individual DMs into the objects and object attributes in the ADM domain.

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

Figure 55: Data Model Importing

During the device model import process:

- The device sends CLI commands to the Device Server, which translates the CLI commands into a DM with device configuration information.
The GUI Server translates the device configuration in the DM into objects and object attributes in the ADM.

The GUI Server then reads the ADM and displays the current information.

Archiving and Restoring

You can archive and restore log and configuration data in NetScreen-Security Manager using standard Unix commands. Logs reside on the Device Server; all other configuration information, including device configuration data, administrators, policies, audit logs, and job information resides on the GUI Server.

Before archiving, you must stop the processes running on both servers, then use the “ls -al” command to identify the actual paths of the GUI Server and Device Server data directories:

- For all information on the GUI Server: /usr/netscreen/GuiSvr/var
- For all information on the Device Server: /usr/netscreen/DevSvr/var

These directories are links representing the paths that were entered at the time the servers were installed.

After archiving, restart the processes on both servers. For details on stopping, starting, and restarting processes on the management system, refer to the NetScreen-Security Manager Installer’s Guide.

Archiving Logs and Configuration Data

To archive log and configuration data:

1. Stop the Device Server and the GUI Server.

2. Use the `ls -al` command to discover the actual paths of the GUI Server and Device Server data directories. These are the directories you need to back up.

   For example:

   ```bash
   ls -al /usr/netscreen/GuiSvr/var
   lrwxrwxrwx 1 root root 21 Feb 25 16:04 /usr/netscreen/GuiSvr/var -> /var/netscreen/GuiSvr
   ```

   The output in the example indicates that the actual location of the GUI Server data is in /var/netscreen/GuiSvr. On your own system, verify where your data is stored and which directories should be backed up. Follow the same procedure to determine the location of your data on the Device Server.

3. Run the appropriate backup command on your Solaris or Linux platform to backup the GUI Server data. For example:
4. Run the appropriate backup command on your Solaris or Linux platform to backup the Device Server data.

For a large amount of log data, using tar may not be appropriate. we recommend using Secure Copy (scp) or File Transfer Protocol (FTP) to backup the Device Server data.

Example using scp:

```
scp -r <local directory> user@host:<remote-directory>
```

Example using FTP:

```
ftp <host name>
b
hash
lcd <local directory>
prompt
mput
```

5. Start GUI Server and Device Server processes.

**Restoring Logs and Configuration Data**

These instructions apply only to systems where the var directory links point to a true location outside the prescribed locations (/usr/netscreen/GuiSvr or /usr/netscreen/DevSvr). We recommend that you do not set these links to point to locations that are inside /usr/netscreen/GuiSvr or /usr/netscreen/DevSvr; doing so can complicate upgrades to NetScreen-Security Manager and requires special precautions during backup and restore procedures.

To restore log and configuration data:

2. Use the mv command to transfer data from the var directories to a safe location. This precaution clears the var directory for restoration of the backups.
3. Untar your backups into both of the locations described above.
The chapters in Part 3 of the NetScreen-Security Manager Administrators Guide are designed to help you create the building blocks of the management system (objects), then configure the Security Policies and VPNs that control your network traffic.

Part 3 contains the following chapters:

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


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

After you have built objects, created Security Policies that define how your devices should handle traffic to and from the firewall, and configured VPNs to connect your network security devices, your network should be configured, connected, and secure. Next, you can begin to use NetScreen-Security Manager’s monitoring, logging, and reporting features to review the status of your security devices (and VPN tunnels) and the efficiency of your firewall and multicast rules, as detailed in Part 4, “Monitoring” on page 513.
Chapter 8
Configuring Objects

Objects represent reusable information, such as network addresses, individual users and user groups, and commonly used configuration data. In NetScreen-Security Manager, objects are shared objects, meaning they are shared between the global domain and all subdomains.

Objects are the building blocks of the NetScreen-Security Manager management system. You can use an object multiple times in the same domain. For example, you can create an address object to represent a host such as an individual workstation, then use the address object in a VPN protected resource and as the source or destination in a firewall or multicast rule.

This chapter contains the following sections:

- About Objects on page 225
- Configuring Address Objects on page 227
- Configuring Schedule Objects on page 232
- Working With DI Attack Objects on page 233
- Working with IDP Attack Objects on page 237
- Configuring Custom DI/IDP Attacks on page 240
- Creating Custom DI Attack Groups on page 258
- Creating Custom IDP Attack Groups on page 259
- Configuring Custom Policy Fields on page 263
- Configuring AntiVirus Objects on page 265
- Configuring Web Filtering Objects on page 270
- Configuring GTP Objects on page 275
- Configuring Service Objects on page 281
- Configuring Authentication Servers on page 289
- Configuring User Objects on page 298
- Configuring VLAN Objects on page 302
- Configuring IP Pools on page 303
- Configuring Group Expressions on page 304
- Configuring Remote Settings on page 307
- Configuring NAT Objects on page 308
- Configuring Certificate Authorities on page 309
- Configuring CRL Objects on page 312
- Configuring Extranet Policies on page 312
- Configuring Protected Resources on page 313
- Configuring IKE Propsals on page 316
About Objects

In the NetScreen-Security Manager UI, most objects appear in the Object Manager; VPN-related objects appear in the VPN Manager. For some object types, such as service objects, attack objects, and IKE proposal objects, predefined objects exist. For most object types, however, you must configure an object before you can use it in your device configuration or Security Policies.

NOTE: If you import an existing device configuration, NetScreen-Security Manager automatically imports all objects defined in the running device configuration.

The Object Manager displays objects created in the current domain only. When working in the global domain, all custom objects are viewable. When working in a subdomain, only custom objects created in the subdomains are viewable. However, when creating an object group, you can select objects from both the current subdomain and global domain. Any global object that is part of a subdomain object group appears within the subdomain object list.

Use the Object Manager to view and configure the following objects:

- Host and network addresses:
  - Address Objects represent individual hosts or subnetworks in your network.
  - NAT Objects (DIP, MIP, VIP) represent references to device-specific NAT configurations (dynamic IPs, mapped IPs, and virtual IPs), enabling multiple devices to share a single object.
  - IP Pools define ranges of IP addresses used to assign an IP address to a RAS user.
  - Remote Settings represents DNS and WINS servers.

- Services and schedules:
  - Schedule Objects represent time periods and determine when a rule is in effect.
  - Service Objects represent predefined and custom network services, such as HTTP/80.

- Application Layer Protection:
  - DI Profiles define the attack signature patterns, protocol anomalies, and the action you want a security device to take against matching traffic.
  - AV Profiles define the server that contains your virus definitions and Antivirus software.
  - Web Filtering Profiles define the URLs, the Web categories, and the action you want a security device to take against matching traffic.

- Users and Authentication:
User Objects represent RAS users on your network.

Authentication Servers represent the servers in your network used to authenticate NetScreen-Security Manager admins, RAS users, and network traffic.

Group Expressions define logical expressions used to include or exclude RAS users.

Certificates:
- Certificate Authority Objects represent the certificate authority’s certificate.
- CRL Objects represent the certificate authority’s certificate revocation list.

VoIP Protection:
- GTP Objects represent client GTP configurations.

Extranet Policies and Custom Policy Fields
- Extranet Policy objects define rules and actions that you may apply to certain traffic on an extranet device (i.e., third-party router).
- Custom Policy Field objects represent metadata information that you can store and use in a structured manner.

Use VPN Manager to view and configure the following objects:
- Protected Resources represent the network components, a network service, and the security device that protects those components and service.
- IKE Phase1 Proposals represent the phase1 proposals used to establish a secure and authenticated communication channel between two VPN members.
- IKE Phase2 Proposals represent the Security Associations for services (such as IPsec) that require key material and/or parameters, as exchanged by two VPN members.

**Importing Objects from Global-PRO**

If you already have objects defined in your existing Juniper Networks NetScreen-Global PRO management system or on the device itself, you can import those objects into NetScreen-Security Manager.

When importing device configurations and their domains from Global PRO, NetScreen-Security Manager also imports all objects that are defined for those domains. During this import process, NetScreen-Security Manager determines if the object is accessible by a single domain or accessible by all domains.

For information about importing objects from Global-PRO, refer to the NetScreen-Security Manager Migration and Installer’s Guide.
Using Objects Across Domains

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

For example, when creating a VPN:

- You can use a global domain user object in a subdomain VPN.
- You can use a subdomain user object in a subdomain VPN.
- You cannot create VPNs across domains. However, you can use an extranet device to represent the device in the other domain to create a cross-domain VPN.
- You cannot use a subdomain user object in a global domain VPN.

When creating a subdomain protected resource, you can include a subdomain address object and a global domain service object, but you can only select the protected resource when you are logged in to that specific subdomain.

Configuring Address Objects

An address object is a representation of a component of your network, such as a workstation, router, switch, subnetwork, or any other object that is connected to your network. You use address book objects in NetScreen-Security Manager to specify the network components you want to protect:

- Firewall and IDP Rules—Use address objects or groups to specify the source and/or destination of network traffic.
- Multicast Rules—Use multicast group address objects to specify the destination of multicast traffic.
- VPNs—Use address objects or groups to create Protected Resources for your Policy-Based and Mixed-Mode VPNs.

Viewing Address Objects

In the navigation tree, click Object Manager > Address Objects to view all address objects for the current domain. You can display Address objects in a tree or table format:

- The Address Tree tab displays address objects in a tree format. To view the members of an Address Object group, click the group to display a member list.
- The Address Table tab displays address objects in a table format with the following columns:
  - Name—Name of the address object
  - Type—Type of the address object (Host, Network, Group)
  - IP/Domain Name—The IP address or host name (such as www.juniper.net) of the address object
Creating Address Objects

You can create the following address objects:

- **Host**—Represents devices, such as workstations or servers, connected to your network.
- **Network**—Represents divisions or subnetworks in your network.
- **Address Object Group**—Represents multiple address objects.
- **Multicast Group**—Represents the destination of multicast packets.

The following sections detail each Address Object type.

Adding a Host Address Object

To add a host address object:

1. In the navigation tree, select **Object Manager > Address Object** to open the address object tree. In the main display area, click the add icon and select **Host**.
2. Enter a unique name for the address object and select a color to represent the address object.
3. Enter a comment about the host (optional).
4. Enter the address that identifies the host on your network:
   - To identify the host with an IP address, select **IP** and enter the IP address of the host. Click **Resolve** to automatically resolve the domain name for that IP address.
   - To identify the host with a domain name, select **Domain Name** and enter the domain name of the host. Click **Resolve** to automatically resolve the IP address for that domain name.
5. Click **OK** to add the address object.

The new host address object immediately appears in the Address Tree and Address Table.

Adding a Network Address Object

To add a network address object:
1. In the navigation tree, open the Object Manager and select **Address Objects** to open the address object tree.

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, then click **OK** to add the address object.

The new network address object immediately appears in the Address Tree and Address Table.

**Editing and Deleting Address Objects**

You can edit a address object by right-clicking on the object and selecting **Edit**. You can also delete a address object by right-clicking on the object and selecting **Delete**. For more information on editing and deleting address objects, refer to the NetScreen-Security Manager Online Help.

**Replacing Address Objects**

You can replace a address object by right-clicking on the object and selecting **Replace With**. Replacing address objects eases the need to make redundant changes to a address object that is referenced in multiple security policies. When replacing address objects however, you want to keep the following in mind:

- there is no validation check when replacing address objects
- you cannot undo or roll back a replace with operation.

**NOTE:** Replacing address objects only applies to those objects in the domain that you are working in.

After replacing address objects, it is good practice to check your security policies for any errors that may result. You can always edit or remove any duplicate objects in the security policy.

**Adding an Address Object Group**

To simplify Security Policies, you can combine multiple address objects in an address object group. An address object group can contain address objects (and other address object groups) from the current subdomain and the global domain.

To add an Address Object Group:

1. In the navigation tree, open the Object Manager and select **Address Objects**. The address object tree appears. In the main display area, click the add icon and select **Group**.
2. Enter a unique name for the group.

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

3. Select a color to represent the group.

4. Enter a comment about the group.

5. In the Non-members list, select the address objects you want to include in the group (hold down Ctrl to select multiple address objects):
   - If you are in the global domain, only the global address objects appear in the non-members list.
   - If you are in a subdomain, both global and subdomain address objects appear in the non-members list.

6. Click Add. The selected address objects now appear in the member list.

7. Click OK to add the group.

You can create address object groups with existing users or create empty address object groups and fill them with users later.

Adding a Multicast Group Address Object

To add a multicast group address object:

1. In the navigation tree, open the Object Manager and select Address Objects. The address object tree appears. In the main display area, click the add icon and select Multicast Group. The New Multicast Group dialog box appears.

2. Enter a name for the multicast group address.

NOTE: Multicast Group address object names must be unique; you cannot assign the same name to another existing multicast group address object.

3. Select a color to represent the multicast group address.

4. Enter a comment about the multicast group address.

5. Enter the IP address of the multicast group.

6. Click OK to add the multicast group address.

Adding Static DNS Host Addresses

This ScreenOS 5.3 feature lets you create a static host name with multiple IP addresses. You can use this feature to create dynamic addressing in NSM.

To add multiple static host addresses:
1. In the navigation tree, open **Device Manager** and click **Security Devices**.

2. Double-click the device you want to configure. The device must be running ScreenOS 5.3 or later.

3. In the navigation tree of the new dialog box, open **Network**, then **DNS**.

4. Click **Settings** to open the Device Settings dialog box.

5. Click the Add icon, enter the host name and host IP address, then click **OK**.

6. Click **OK** to save the changes and close the dialog box.

**Example**

In some cases, a common firewall policy is desired but due to differences in the IP addressing at different sites, it is impossible to share the policy. Using static host entries and address objects, a policy can be shared. Each device contains a local mapping of hostname to IP, but the policy references an address object by hostname. This allows the firewall policy to focus on the application as opposed to the specific IP addressing.

For example, each site might have a web server, each with a different IP address. By defining an address object using the hostname "webserver" and then using that object in the firewall policy, the device will resolve the address object's hostname to the correct IP for that device (as defined by the static host entry of each device).

1. In the navigation tree, open **Object Manager** and click **Address Objects**.

2. Click the **Add** icon then select **Host** to open the New Host dialog box.

3. Enter the same name in the Name field that you entered for the Device host name in the previous section. These values are case sensitive and must match exactly.

4. Click **OK** to save the name and close the dialog box.

5. Return to the navigation tree, open **Security Policy**.

6. Click the **Add** icon and enter the security policy name, then click **OK**.
7. Double-click the name of the security policy you just created.

8. Right-click the value in the Source column or the Destination column.

9. Select the address object you just created, click Add, then click OK. When the address object is pushed to a device, the host name resolves dynamically. One policy can be assigned to multiple devices.

**Blocked Hosts**

NSM can block the IP address of hosts where login attempts fail consecutively for a specified number of times. The default value is 5 times. NSM saves a list of these blocked IP addresses. Go to Tools > Managed Blocked Hosts to display a list of blocked hosts or to clear the blocked IP addresses. If the local host is blocked, you must use another computer to use this option to unblock the host IP address.

**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).

Working With DI Attack Objects

Deep Inspection (DI) attack objects contain attack patterns and protocol anomalies for known attacks and unknown attacks that attackers can use to compromise your network. However, DI attack objects don’t work on their own—they need to be part of an attack object group, and a DI Profile object before you can use them in a firewall rule to detect known attacks and preventing malicious traffic from entering your network.

To create a Deep Inspection (DI) Profile object, you add predefined attack object groups (created by Juniper Networks) and/or your own custom attack object groups to the Profile object. After creating the DI Profile, you add the Profile object in the Rule Option column of a firewall rule. If an attack is detected, the device generates an attack log entry that appears in the Log Viewer.

For information about creating your own custom attack objects and custom attack object groups, see “Working With DI Attack Objects” on page 233. For information about configuring Deep Inspection in a firewall rule, see “Creating DI Profiles” on page 235. For information about attack log entries, see “Deep Inspection Alarm Log Entries” on page 708.
Viewing Predefined DI Attack Objects

NetScreen-Security Manager contains a database of hundreds of predefined DI attack objects designed to protect networks from multiple attack vectors. Predefined groups contain attack objects, which you can use in a DI Profile to match traffic against known and unknown attacks.

NOTE: NetScreen-Security Manager displays a superset of all predefined DI attack objects. Based on the platform and ScreenOS firmware version, security devices include a specific subset of DI attack objects. Therefore, the list of predefined DI attack objects displayed in the NetScreen-Security Manager UI might not match the list of predefined DI attack objects on the physical security device.

To view individual predefined attack objects, in Object Manager, select Attack Objects > DI Objects. The Predefined Attacks tab (default view) displays a table of predefined attack objects that represent known and unknown attack patterns. Use the Predefined Attacks tab to quickly view details about an attack object, such as name of the attack object, attack severity, attack category, and attack references. To view the properties for an attack, right-click the attack and select View.

To locate all firewall rules that use a predefined attack object or group, right-click the attack object and select View Usages.

Viewing Attack Version Information for Attack Objects

You can view details for predefined attack objects; however, not all details are applicable to all attacks.

The Pattern field under the Detection tab in the Attack Version dialog box contains the regular expression used to identify the attack. Juniper Networks Security Engineering might choose to hide the exact pattern for specific attack objects. This is done to protect the confidentiality of either the source or target of the specific attack object. In such cases, the field displays Protected instead of the regular expression.

To view attack version information, click one of the Supported Platform links within an attack object dialog box.

Viewing Predefined DI Attack Object Groups

To view predefined attack object groups, in Object Manager, select Attack Objects > DI Objects, then select the Predefined Attack Groups tab. The name of each attack object group indicates the severity, protocol, and attack type of the individual attack objects contained within. For example, the predefined attack object group CRITICAL:DNS:ANOMALY contains predefined protocol anomaly attack objects that detect critical Domain Name Service (DNS) attacks.

To locate all firewall rules that use a predefined attack object or group, right-click the attack object group and select View Usages.
Updating Predefined DI Attack Objects and Groups

You cannot create, edit, or delete predefined DI attack objects or groups, but you can update the attack object database with new attack objects created by Juniper Networks. Updates can include:

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

For information about managing the attack object database, see “Managing the Attack Database” on page 197.

Creating DI Profiles

A Deep Inspection (DI) Profile object contains predefined attack object groups (created by Juniper Networks), and/or your own custom attack object groups. After creating the DI Profile, you add the Profile object in the Rule Option column of a firewall rule.

To create a DI Profile, in the navigation tree, select Object Manager > Attack Objects > DI Objects, then click the Profile tab. Click the Add icon to add a new Profile object, then configure the name, color, and comments for profile object as desired. To add members to the profile object, configure the following:

- DI Severity Setting—Select a DI Severity setting for the profile object. The DI Severity setting overrides the severity setting of the attack objects included in each profile member.

- Signature Category—Select a category of DI signatures. You can only select categories for which you have a license.

Categories are as follows:

- Server Protection Pack—Designed to protect servers.
- Client Protection Pack—Designed to protect remote and home offices.
- Worm Mitigation Pack—Designed to protect against worms.
- Base (Default) Pack—All signatures. Might be too large for some devices.

- DI Attack Objects and Groups—Add a profile member to the profile object. Each profile member can contain attack object groups, and you can add multiple profile members to the profile object. Within each profile member:

  - Select the attack object groups you want to include in this profile member.
  - Configure the action you want the security device to take when an attack object within the profile member matches traffic. Table 19 lists DI profile actions.
Table 19: Deep Inspection Profile Actions

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>The security device takes no action against the connection.</td>
</tr>
<tr>
<td>ignore</td>
<td>The security device ignores the remainder of a connection after an attack object is matched.</td>
</tr>
<tr>
<td>drop packet</td>
<td>The security device drops a matching packet before it can reach its destination but does not close the connection. Use this action to drop packets for attacks in traffic that is prone to spoofing, such as UDP traffic. Dropping a connection for such traffic could result in a denial of service that prevents you from receiving traffic from a legitimate source IP address. For TCP connections, dropping a single packet will result in the same packet being resent. So, Drop Packet settings are translated to Drop Connection settings for TCP connections.</td>
</tr>
<tr>
<td>drop connection</td>
<td>The security device drops the connection without sending a RST packet to the sender, preventing the traffic from reaching its destination. Use this action to drop connections for traffic that is not prone to spoofing.</td>
</tr>
<tr>
<td>close client and server</td>
<td>The security device closes the connection and sends a RST packet to both the client and the server.</td>
</tr>
<tr>
<td>close client</td>
<td>The security device closes the connection to the client but not to the server.</td>
</tr>
<tr>
<td>close server</td>
<td>The security device closes the connection to the server but not to the client.</td>
</tr>
</tbody>
</table>

NOTE: Network security is an ongoing process of defining 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, set an alert for the event, or use all three methods.

- Configure Deep Inspection Alerts. Enable this option to create an event log entry for matching traffic. If the security device matches network traffic to an attack object in the rule, NetScreen-Security Manager creates an event log entry that describes that attack (direction, service, and Attack object) and displays an alert in the Log Viewer.

- Configure IP Action. Enable this option to direct the device to take action against a brute force attack. When enabled, configure the following IP controls action:
  - Action. Select the action you want the device to take when it detects a brute force attack. Table 20 lists DI IP actions.

Table 20: Deep Inspection IP Actions

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Block</td>
<td>The security device logs the event and drops all further traffic matching the target definition for the period of time specified in the timeout setting.</td>
</tr>
</tbody>
</table>
### Target
Specifies a set of elements that must match for the security device to consider a packet part of a brute force attack. The specified set of elements in an IP packet arriving during a specified timeout period must match that in the packet that the security detected as part of a brute force attack for the subsequent packet to be considered part of the same attack. Possible values are Source, Destination, Destination Port and Protocol; Source; Destination; From Zone, Destination, Destination Port and Protocol; and From Zone.

### Timeout (sec)
A period of time following brute force attack detection during which the security device performs an IP action on packets matching specified target parameters. The default is 60 seconds.

After you have created the DI Profile object, you can use the object in your firewall rules. For details, see “Configuring a DI Profile/Enable IDP For Firewall Rules” on page 345.

### Working with IDP Attack Objects

NetScreen-Security Manager contains a database of predefined IDP attack objects and IDP attack object groups that you can use in Security Policies to match traffic against known and unknown attacks. Juniper Networks updates the predefined attack objects and groups on a regular basis with newly-discovered attack patterns.

### Viewing Predefined IDP Attacks
The Predefined Attacks tab displays all attacks in a table format and includes the following information:

- Name of the attack object
- Severity of the attack: critical, major, minor, warning, info
- Category
- Keywords for the attack
- CVE number which identifies the attack’s number in the Common Vulnerabilities and Exposures database
- Bugtraq number which identifies the equivalent attack in the Security Focus Bugtraq database
By default, attack objects are listed alphabetically by Category name. To view attacks in a different order, click a column heading. To display a detailed description of an attack object, double-click the attack.

To view attack object details, right-click the attack object and select View. Figure 56 shows the attack viewer.

See Configuring Custom DI/IDP Attacks on page 240 for field descriptions.

Figure 56: Attack Viewer
Viewing Predefined IDP Attack Groups

The Predefined Attack Group tab displays the following predefined attack groups:

- **All** — a list of all attack objects, organized in the categories described below.
- **Recommended** — a list of all attack object objects that Juniper Networks considers to be serious threats, organized into categories.
- **Attack Type** groups attack objects by type (anomaly or signature). Within each type, attack objects are grouped by severity.
- **Category** groups attack objects by predefined categories. Within each category, attack objects are grouped by severity.
- **Operating System** groups attack objects by the operating system to which they apply: BSD, Linux, Solaris, or Windows. Within each operating system, attack objects are grouped by services and severity.
- **Severity** groups attack objects by the severity assigned to the attack. IDP has five severity levels: Info, Warning, Minor, Major, Critical. Within each severity, attack objects are grouped by category.

To locate all rules that use a predefined attack object group, right-click the attack object group and select **View Usages**.

A predefined static group can include the following members:

- Predefined attack objects
- Predefined static groups
- Predefined dynamic groups

To display a detailed description of an attack object group, double-click the attack.

Viewing Attack Version Information for Attack Objects and Groups

NetScreen-Security Manager lets you look at the details of predefined attack objects and groups. Not all details are applicable to all attacks.

The Pattern field under the Detection tab in the Attack Version dialog box contains the regular expression used to identify the attack. Juniper Networks Security Engineering may choose to hide the exact pattern for specific attack objects. This is done to protect the confidentiality of either the source or target of the specific attack object. In such cases, the field displays Protected instead of the regular expression.

To view attack version information, click one of the Supported Platform links within an attack object dialog box.
Updating Predefined IDP Attack Objects and Groups

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

NOTE: You cannot create, edit, or delete predefined attack object or groups.

Updates to the attack object database can include:

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

For information about updating the attack object database, see “Managing the Attack Database” on page 197

Configuring Custom DI/IDP Attacks

You can create custom DI and IDP attack objects to detect new attacks or customize copies of existing attack objects to meet the unique needs of your network. For example, you might want to edit the context of a custom attack object that is producing too many false positives on your network, or you might want to create a new custom attack object to detect the latest virus or Trojan that is sweeping the Internet.

The attack object creation process is similar for custom DI and IDP attack objects. To create both object types, you use the Attack Object Wizard to enter attack object information, attack pattern, and other important information. After you have configured the object however, you use each object differently:

- To use a custom DI attack object to protect your network, you must add the object to a custom attack object group and then a DI Profile object, which you then select within the Rule Options of a firewall rule. For information about creating a custom attack object group, see “Creating Custom IDP Attack Groups” on page 259. For information about creating a DI Profile object, see “Creating DI Profiles” on page 235.

- To use a custom IDP attack object to protect your network, you can add the attack object in an IDP rule.

Using the Attack Object Wizard

To help you create custom attack objects, NetScreen-Security Manager UI uses a Custom Attack Object wizard to guide you through each step. During the creation process, the wizard prompts you for:
Chapter 8: Configuring Objects

- **Attack Object information**—You must supply an attack object name and configure the target platforms that support the attack object. You can also create an attack description, enter attack references, and set a severity for the attack object, if desired. The following sections detail the general attack object information fields.

- **Attack Version information**—After you have selected the target platforms, you must supply information about the attack version, including the protocol and context used to perpetrate the attack. When the attack is considered malicious, the direction and flow of the attack, the signature pattern of the attack, and the values found in the header section of the attack traffic.

To create a custom attack object, from the main navigation tree, select **Object Manager > Attack Objects > DI Objects** or **IDP Objects**, then select the Custom Attacks tab. Click the Add icon to display the custom attack object wizard.

**Copying/Editing Predefined Attack Objects to Create Custom Attack Objects**

You can also make a copy of a predefined attack object. This copy is a custom attack object, which you can modify like any other custom object. The copy must have a different name than the original, predefined attack object.

To create a custom version of a predefined attack object, open an existing predefined attack object, and click the Edit button in the Attack Viewer. A new attack object with the same parameters as the existing predefined attack object appears. The new object has the same name as the previous object, but with “-Copy” appended. After editing the parameters that you want, click **OK**.

The following sections explain the attack object creation process; for instructions for creating a custom attack object, see the NetScreen-Security Manager Online Help topic “Creating Custom Attack Objects”. The fields that can be modified are described below.

**Configuring Attack Name and Description**

In the Attack Name and Description tab, enter basic information about the attack, such as the attack object name and attack severity. You can also enter additional information, such as a general description and keywords, which can make it easier for you to locate and maintain the attack object as you use it in your firewall rules. Specifically, the attack object wizard prompts you for the following:

- **Name**—Enter an alphanumeric name for the object. You might want to include the protocol the attack uses in the attack name.

- **Description**—Enter important information about the attack, such as why you created the attack object, how the attack or exploit works, and what specific systems on your network the attack object is intended to protect. For example, you might want to include the following information:
  - Attack type (buffer overflow, password exploit, format string attack, denial-of-service)
  - Affected system (hardware, operating system, software application, or protocol the attack targets)
- Attack mechanism (how the attack works)
- Attack lethality (the consequences of a successful attack)

You are not required to include all this information when creating a new custom Attack Object, but it’s a good idea. If you ever need to edit this attack object, the description can help you remember important information about the attack.

- Severity—Select the severity that matches the lethality of this attack on your network. Severity categories, in order of increasing lethality, are: info, warning, minor, major, critical. Critical attacks are the most dangerous—typically these attacks attempt to crash your server or gain control of your network. Informational attacks are the least dangerous, and typically are used by network administrators to discover holes in their own security system.

- Category—Enter the category to which the attack object belongs.

- Keywords—Enter descriptive words or numbers associated with the attack. Later, after you have added the custom attack object to the database, you can search using these keywords to quickly locate the attack.

- Recommended—Check this checkbox if you want this attack object to be part of your highest-risk set of attack objects. Later, when you add this attack object to dynamic groups, you can specify whether only Recommended attack objects will be included.

- Recommended Action—This field only exists in pre-defined attack objects. When you use an attack object in a policy, you can specify what action the IDP device should take when it detects the attack. However, for IDP-capable devices running IDP 4.1 and later or ScreenOS 6.0 or later, you can tell the device to use the action recommended by Juniper Networks for that attack.

When you have completed entering the basic attack information, you are ready to enter the extended attack information.

**Configuring Extended Information**

In the Extended Information tab, enter specific information about the attack. Specifically, the attack object wizard prompts you for the following:

- Impact—Enter details about the impact of a successful attack, including information about system crashes and access granted to the attacker.

- Description—Enter details about how the attack works. You might also consider adding information on the attack history (such as how it attacked your network and what steps you took to neutralize the threat).

- Tech Info—Enter information about the vulnerability, the commands used to execute the attack, which files are attacked, registry edits, and other low-level information.
- Patches—List any patches available from the product vendor, as well as information on how to prevent the attack. You might find this information in a network security advisory or from the product vendor.

NOTE: Use HTML tags to include a hyperlink within the text.

When you have completed entering the extended attack information, you are ready to enter the external references.

**Configuring External References**

In the External References tab, enter the external references, such as links to the security community’s official descriptions of an attack, you used when researching the attack.

External references, in conjunction with standard network security references, can help other admins get more information about how an attack works or help you research and compare the attack in relation to a suspected new attack.

Specifically, the attack object wizard prompts you for the following:

- **URLs**—Enter up to three URLs for external references you used when researching the attack.

- **Standard References**—Enter the standardized network security organizations’ attack designations for the attack:
  - CVE (Common Vulnerabilities and Exposures) is a standardized list of vulnerabilities and other information security exposures. The CVE number is an alphanumeric code, such as CVE-1999-0003
  - BugTraq is a moderated mailing list that discusses and announces computer security vulnerabilities. The BugTraq ID number is a three-digit code, such as 831 or 120.

When you have completed entering the external references for the attack, you are ready to select the target platforms for the attack object.

**Configuring Target Platforms**

In the Target Platform tab, you must select the target platform, configure the attack version, then set a direction filter (described on page 258) for the attack object. To select the target platform and configure the attack version, click the Add icon to display the Attack Version Wizard.

First, you must select the ScreenOS or IDP versions for which the attack object is designed. Because different versions of ScreenOS and IDP support additional functionality than previous versions, you must specify the versions that must support the attack object.
To configure the selected target platform, click the Add icon to display the New Supported Platform dialog box. Select the versions of ScreenOS (sos5.0.0, sos5.1.0, sos5.2.0) or IDP (idp4.0.0) that must support the attack object. After you have made your selection, the attack object wizard automatically removes options from the custom attack object creation process based on the selected target platforms.

NOTE: The string “isp-sos” in a Target Platform label indicates ScreenOS software that also has IDP capability, such as the software that runs on an ISG 2000.

The string “idp” (without the “sos”) in the Target Platform label indicates software that runs on a standalone IDP device, such as an IDP 600C.

Next, select the type of attack that the attack object detects. After you have added the supported platform to the custom attack object, you can configure the attack type on that platform. Select from one of the following attack types:

- **Signature Attack Object**—(DI and IDP attack objects) A signature attack object uses a stateful attack signature (a pattern that always exists within a specific section of the attack) to detect known attacks. Stateful signature attack objects also include the protocol or service used to perpetrate the attack and the context in which the attack occurs. If you know the exact attack signature, the protocol, and the attack context used for a known attack, select this option. For more information about creating a signature attack object, see “Creating a Signature Attack Object” on page 245.

- **Protocol Anomaly Attack Object**—(IDP attack objects only) A protocol anomaly attack object detects unknown or sophisticated attacks that violate protocol specifications (RFCs and common RFC extensions). You cannot create new protocol anomalies, but you can configure a new attack object that controls how the security device handles a predefined protocol anomaly when detected. If you don’t know that exact attack signature, but you do know the protocol anomaly that detects the attack, select this option. For more information about creating a protocol anomaly attack object, see “Configuring a Protocol Anomaly Attack Object” on page 255.

- **Compound Attack Object**—(IDP attack objects only) A compound attack object detects attacks that use multiple methods to exploit a vulnerability. This object combines multiple signatures and/or protocol anomalies into a single attack object, forcing traffic to match a pattern of combined signatures and/or anomalies within the compound attack object before traffic is identified as an attack. By combining and even specifying the order in which signatures or anomalies must match, you can be very specific about the events that need to take place before the security device identifies traffic as an attack. For more information about creating a compound attack object, see “Configuring a Compound Attack Object” on page 255.

If you need to detect an attack that uses several benign activities to attack your network, or if you want to enforce a specific sequence of events to occur before the attack is considered malicious, select this option.
Click Next to configure the attack version information for the signature attack object. You must enter some general information about attack version and specific details about the attack pattern, such as the protocol and context used to perpetrate the attack. When using a packet-related context, you can also define IP settings and protocol header matches for the attack version.

Creating a Signature Attack Object

When you configure a signature attack object, you enter important information about the protocol and context used to perpetrate the attack, when the attack is considered malicious, the direction and flow of the attack, the signature pattern of the attack, and the values found in the header section of the attack traffic.

Configuring General Attack Properties

In the general properties screen, you can define the false positive frequency for the attack version, the service that the attack uses to enter your network, and the time parameters (scope and count) that determine when a traffic abnormality is identified as an attack. The following sections detail the attack version general properties.

Configuring False Positives

Select a false positive setting that indicates the frequency (unknown, rarely, occasionally, frequently) the attack object produces a false positive on your network. Although you might not have this information when you initially configure the custom attack object, as you fine-tune your system to your network traffic you can change this setting to help you track false positives.

Configuring Service Binding (IDP Attack Objects Only)

For IDP attack objects, select the service that the attack uses to enter your network. You must select a service other than “Any” if you want to specify a service context for the attack object.

NOTE: For DI attack objects, you do not select a service binding.

- Any—If you are unsure of the correct service, select Any and DI attempts to match the signature in all services. Because some attacks use multiple services to attack your network, you might want to select the Any service binding to detect the attack regardless of which service the attack chooses for a connection.

- IP—If you are not sure of the correct service but know the IP protocol type, select IP protocol type for the service binding. You can specify the name of the protocol type, or the protocol type number. If you select IP as the service type, you should also specify an attack pattern (in the Detection area) and IP settings values (in the IP area). Additionally, if you use a context binding of first packet, you must leave the attack pattern empty. Table 21 lists the supported protocol types.
ICMP, TCP, and UDP—Attacks that do not use a specific service might use a specific protocol to attack your network. Some TCP and UDP attacks use standard ports to enter your network and establish a connection; to detect these attack, configure the firewall rule that contains this attack object to monitor traffic on the standard service port or ICMP ID.

RPC—The remote procedure call (RPC) protocol is used by distributed processing applications to handle interaction between processes remotely. When a client makes a remote procedure call to an RPC server, the server replies with a remote program; each remote program uses a different program number. To detect attacks that use RPC, configure the service binding as RPC and specify the RPC program ID.

Service—Most attacks use a specific service to attack your network. If you select Service as the service binding, you must select the specific service used to perpetrate the attack. Additionally, you are restricted to general attack contexts (packet, first packet, stream, stream 256, or line context). To detect these attacks, configure the service binding to match the attack service. See Table 22.

Supported Services:

---

Table 21: IP Protocol Name and Type Numbers

<table>
<thead>
<tr>
<th>Protocol Name</th>
<th>Protocol Type Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP</td>
<td>2</td>
</tr>
<tr>
<td>IPIP</td>
<td>4</td>
</tr>
<tr>
<td>EGP</td>
<td>8</td>
</tr>
<tr>
<td>PUP</td>
<td>12</td>
</tr>
<tr>
<td>TP</td>
<td>29</td>
</tr>
<tr>
<td>IPV6</td>
<td>41</td>
</tr>
<tr>
<td>ROUTING</td>
<td>43</td>
</tr>
<tr>
<td>FRAGMENT</td>
<td>44</td>
</tr>
<tr>
<td>RSVP</td>
<td>46</td>
</tr>
<tr>
<td>GRE</td>
<td>47</td>
</tr>
<tr>
<td>ESP</td>
<td>50</td>
</tr>
<tr>
<td>AH</td>
<td>51</td>
</tr>
<tr>
<td>ICMPV6</td>
<td>58</td>
</tr>
<tr>
<td>NONE</td>
<td>59</td>
</tr>
<tr>
<td>DSTOPTS</td>
<td>60</td>
</tr>
<tr>
<td>MTP</td>
<td>92</td>
</tr>
<tr>
<td>ENCAP</td>
<td>98</td>
</tr>
<tr>
<td>PIM</td>
<td>103</td>
</tr>
<tr>
<td>COMP</td>
<td>108</td>
</tr>
<tr>
<td>RAW</td>
<td>255</td>
</tr>
</tbody>
</table>
Table 22: Supported Services for Service Bindings

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
<th>Default Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIM</td>
<td>AOL Instant Messenger</td>
<td>TCP/19, UDP/19</td>
</tr>
<tr>
<td>Chargen</td>
<td>Chargen</td>
<td></td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
<td>TCP/9, UDP/9</td>
</tr>
<tr>
<td>Discard</td>
<td>Discard</td>
<td>TCP/7, UDP/7</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name Service</td>
<td>TCP/53, UDP/53</td>
</tr>
<tr>
<td>Echo</td>
<td>Echo</td>
<td>TCP/7, UDP/7</td>
</tr>
<tr>
<td>Finger</td>
<td>Finger Information Protocol</td>
<td>TCP/79, UDP/79</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
<td>TCP/21, UDP/21</td>
</tr>
<tr>
<td>Gnutella</td>
<td>Gnutella</td>
<td></td>
</tr>
<tr>
<td>Gopher</td>
<td>Gopher</td>
<td></td>
</tr>
<tr>
<td>HTTP</td>
<td>Hypertext Transfer Protocol</td>
<td>TCP/80, UDP/80</td>
</tr>
<tr>
<td>ICMP</td>
<td>Internet Control Message Protocol</td>
<td>TCP/113</td>
</tr>
<tr>
<td>IDENT</td>
<td>IDENT</td>
<td></td>
</tr>
<tr>
<td>IMAP</td>
<td>Internet Message Access Protocol</td>
<td>TCP/143, UDP/143</td>
</tr>
<tr>
<td>IRC</td>
<td>Internet Relay Chat</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
<td></td>
</tr>
<tr>
<td>lpr</td>
<td>Line Printer spooler</td>
<td></td>
</tr>
<tr>
<td>MSN</td>
<td>Microsoft Instant Messenger</td>
<td></td>
</tr>
<tr>
<td>NBName</td>
<td>NetBios Name Service</td>
<td>UDP/137 (NBName)</td>
</tr>
<tr>
<td>NBDS</td>
<td></td>
<td>UDP/138 (NBDS)</td>
</tr>
<tr>
<td>NFS</td>
<td>Network File System</td>
<td></td>
</tr>
<tr>
<td>nntp</td>
<td>Network News Transfer Protocol</td>
<td></td>
</tr>
<tr>
<td>NTP</td>
<td>Network Time Protocol</td>
<td></td>
</tr>
<tr>
<td>POP3</td>
<td>Post Office Protocol, Version 3</td>
<td>TCP/110, UDP/110</td>
</tr>
<tr>
<td>Portmapper</td>
<td>Portmapper</td>
<td>TCP/111</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Remote Authentication Dial In User Service</td>
<td></td>
</tr>
<tr>
<td>rexec</td>
<td>Rexec</td>
<td></td>
</tr>
<tr>
<td>rlogin</td>
<td>rlogin</td>
<td>TCP/513</td>
</tr>
<tr>
<td>rsh</td>
<td>rsh</td>
<td></td>
</tr>
<tr>
<td>rtsp</td>
<td>rtsp</td>
<td></td>
</tr>
<tr>
<td>SMB</td>
<td>Server Message Block</td>
<td></td>
</tr>
<tr>
<td>SMTP</td>
<td>Simple Mail Transfer Protocol</td>
<td>TCP/25, UDP/25</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
<td>TCP/161, UDP/161</td>
</tr>
<tr>
<td>SNMPTRAP</td>
<td>SNMP trap</td>
<td>TCP/162, UDP/162</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell</td>
<td>TCP/22, UDP/22</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer</td>
<td></td>
</tr>
<tr>
<td>syslog</td>
<td>Syslog</td>
<td>UDP/514</td>
</tr>
<tr>
<td>Telnet</td>
<td>Telnet TCP protocol</td>
<td>TCP/23, UDP/23</td>
</tr>
</tbody>
</table>
Configuring Custom DI/IDP Attacks

Use Time Binding to configure the time attributes for the custom attack object. Time attributes control how the attack object identifies attacks that repeat for a certain number of times. By configuring the scope and count of an attack, you can detect a sequence of the same attacks over a period of time (one minute) across sessions.

After you enable Time Binding, configure the following time attributes:

- **Scope**—Select the scope within which the count occurs:
  - Source. Select this option to detect attacks from the source IP address for the specified number of times, regardless of the destination IP address.
  - Destination. Select this option to detect attacks to the destination IP address for the specified number of times, regardless of the source IP address.
  - Peer. Select this option to detect attacks between source and destination IP addresses of the sessions for the specified number of times.

- **Count**—Enter the number of times that the attack object must detect an attack within the specified Scope before the device considers the attack object to match the attack. For example, the TCP Protocol Anomaly “Segment Out of Window” is harmless and is occasionally seen on networks. Thousands of these anomalies between given peers, however, is suspicious.

If you bind the attack object to multiple ports (see “Configuring Attack Detection Properties” on page 248), and the attack object detects that attack on different ports, each attack on each port is counted as a separate occurrence. For example, when the attack object detects that attack TCP/80 and then on TCP/8080, the count is two.

After you finish entering the general attack properties for the attack type, click **Next** to configure the attack detection properties.

### Configuring Attack Detection Properties

In the Attack Pattern screen, you can define the signature pattern of the attack, the context in which the attack occurs, and the direction and flow of the attack.
Configuring Attack Pattern

The attack pattern is the signature of the attack you want to detect. A signature is a pattern that always exists within an attack; if the attack is present, so is the signature. To create the attack pattern, you must first analyze the attack to detect a pattern (such as a segment of code, a URL, or a value in a packet header), then create a syntactical expression that represents that pattern. Table 23 lists the syntax based on regular expressions to match signature patterns for DI and IDP.

Table 23: Attack Pattern Syntax

<table>
<thead>
<tr>
<th>Pattern</th>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct binary match (octal)</td>
<td>\0&lt;octal-number&gt;</td>
</tr>
<tr>
<td>Direct binary match (hexadecimal)</td>
<td>\X&lt;hexadecimal-number&gt; \X</td>
</tr>
<tr>
<td>Case insensitive matches</td>
<td>[&lt;character-set&gt;]</td>
</tr>
<tr>
<td>Match any symbol</td>
<td>.</td>
</tr>
<tr>
<td>Match 1 or more symbols</td>
<td>*</td>
</tr>
<tr>
<td>Match 0 or 1 symbols</td>
<td>?</td>
</tr>
<tr>
<td>Grouping of expressions</td>
<td>(</td>
</tr>
<tr>
<td>Alternation, typically used with ( )</td>
<td></td>
</tr>
<tr>
<td>Character range</td>
<td>[&lt;start&gt;-&lt;end&gt;]</td>
</tr>
<tr>
<td>Negation of range</td>
<td>[^&lt;start&gt;-&lt;end&gt;]</td>
</tr>
</tbody>
</table>

NOTE: Regular expression support is provided by the PCRE library package, which is open source software, written by Philip Hazel, and copyright by the University of Cambridge, England. The source software is available using FTP from the following web site: ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/

Table 24 lists some example syntax matches.

Table 24: Attack Pattern Syntax Example Matches

<table>
<thead>
<tr>
<th>This Syntax</th>
<th>Matches...</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>\01 86 A5 00 00\X</td>
<td>the five specified bytes verbatim.</td>
<td>01 86 A5 00 00</td>
</tr>
<tr>
<td>(hello</td>
<td>world)</td>
<td>hello or world.</td>
</tr>
<tr>
<td>(hello</td>
<td>world)+</td>
<td>hello or world one or more times.</td>
</tr>
<tr>
<td>[hello]</td>
<td>hello in a case insensitive manner.</td>
<td>hElLo HEIIo heLLO</td>
</tr>
</tbody>
</table>
Configuring Attack Context

Select the context that defines the location of the signature.

**NOTE:** For IDP attack objects, if you selected “Any” as the Service Binding in the Attack Pattern screen, you cannot select a service context here.

If you know the service and the specific service context, select that service then select the appropriate service contexts. If you know the service, but are unsure of the specific service context, select **Other** then select one of the following general contexts:

**NOTE:** If you select a line, stream, stream 256, or a service context, you cannot specify IP header contents (in the Header Match screen).

- Select packet context to match the attack pattern within a packet. When you select this option, you should also specify the Service Binding (in the General tab) and define the service header options (in the Header Match tab). Although not required, specifying these additional parameters helps to improve the accuracy of the attack object and can improve performance.

- Select first packet context detect the attack in only the first packet of a stream. When the flow direction for the Attack Object is set to any, the security device checks the first packet of both the server-to-client (STC) and client-to-server (CTS) flows. If you know that the attack signature appears in the first packet of a session, choosing first packet instead of packet reduces the amount of traffic the security device needs to monitor, which improves performance.

- Select stream context to reassemble packets and extract the data to search for a pattern match. However, a security device does not recognize packet boundaries for stream contexts, so data for multiple packets is combined. Select this option only when no other context option contains the attack.

### Syntax Table

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Matches...</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>[c-e]a(d</td>
<td>t)</td>
<td>Anything with the first letter of c, d, or e, the middle letter a and ending in d or t.</td>
</tr>
<tr>
<td>[^c-d]a(d</td>
<td>t)</td>
<td>Expressions that begin with a letter other than c, d, or e, have the second letter a, and end in d or t.</td>
</tr>
<tr>
<td>a*b+c</td>
<td>Any number of “a” characters followed by one or more b characters followed by a c.</td>
<td>bc, abc, aaaabbbbc</td>
</tr>
</tbody>
</table>

To negate the pattern, enable **Negate**.
Select stream 256 context to reassemble packets and search for a pattern match within the first 256 bytes of a traffic stream. When the flow direction is set to any, the security device checks the first 256 bytes of both the STC and CTS flows. If you know that the attack signature will appear in the first 256 bytes of a session, choosing stream 256 instead of stream reduces the amount of traffic that the security device must monitor and cache, improving performance.

Select line context to detect a pattern match within a specific line within your network traffic.

Configuring Attack Direction
Select the connection direction of the attack. Using single direction (instead of Any) improves performance, reduces false positives, and increases detection accuracy:

- Client to Server (detects the attack only in client-to-server traffic)
- Server to Client (detects the attack only in server-to-client traffic)
- Any (detects the attack in either direction)

Configuring Attack Flows
Select the connection flow of the attack. Using a single flow (instead of Both) improves performance and increases detection accuracy.

- Control (detects the attack in the initial connection that is established persistently to issue commands, requests, and so on.)
- Auxiliary (detects the attack in the response connection established intermittently to transfer requested data)
- Both (detects the attack in the initial and response connections)

After you finish entering the attack detection properties for the attack type, click Next to configure the attack IP settings and protocol headers.

Configuring Header Match Properties
Specify specific values and options that exist within the header of the attack packet.

NOTE: You can configure header values only for attack objects that use a packet or first packet context. If you selected a line, stream, stream 256, or a service context (in the Detection tab) you cannot specify header contents.

If you are unsure of the options or flag settings for the malicious packet, leave all fields blank and the security device attempts to match the signature for all header contents. For each value you enter, you must specify the relational or equality operator. Table 25 lists DI attack header match modifiers.
Table 25: DI Attack Header Match Modifiers

<table>
<thead>
<tr>
<th>Modifier</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>==</td>
<td>equal to</td>
</tr>
<tr>
<td>!=</td>
<td>not equal to</td>
</tr>
<tr>
<td>&gt;</td>
<td>greater than</td>
</tr>
<tr>
<td>&lt;</td>
<td>less than</td>
</tr>
</tbody>
</table>

Additionally, for each flag you must specify whether or not a flag is configured (none), the flag is set (set), or the flag is not set (unset).

**Configure IP Header Matches**

In the IP tab, for attacks that use IP and a packet context, you can set values for the following IP fields and flags:

- **Type of Service**—Specify an operand (none, =, !, >, <) and a decimal value for the service type. Common service types are:
  - 0000 Default
  - 0001 Minimize Cost
  - 0002 Maximize Reliability
  - 0003 Maximize Throughput
  - 0004 Minimize Delay
  - 0005 Maximize Security

- **Total Length**—Specify an operand (none, =, !, >, <) and a decimal value for the number of bytes in the packet, including all header fields and the data payload.

- **ID**—Specify an operand (none, =, !, >, <) and a decimal value for the unique value used by the destination system to reassemble a fragmented packet.

- **Time to Live**—Specify an operand (none, =, !, >, <) and a decimal value for the time-to-live (TTL) value of the packet. This value represents the number of routers the packet can pass through. Each router that processes the packet decrements the TTL by 1; when the TTL reaches 0, the packet is discarded.

- **Protocol**—Specify an operand (none, =, !, >, <) and a decimal value for the protocol used.

**NOTE:** The Protocol field does not appear for DI attack objects.

- **Source**—Enter the source IP of the attacking device.
- **Destination**—Enter the destination IP of the attack target.
Reserved Bit—This bit is not used.

More Fragments—When set (1), this option indicates that the packet contains more fragments. When unset (0), it indicates that no more fragments remain.

Don’t Fragment—When set (1), this option indicates that the packet cannot be fragmented for transmission.

**Configuring TCP Header Matches**

For attacks that use TCP and a packet context, in the Protocol tab, select TCP Packet Header Fields from TCP/UDP/ICMP Header Matches menu, then set values for the following TCP fields and flags:

- **Source Port**—Specify an operand (none, =, !, >, <) and a decimal value for the port number on the attacking device.

- **Destination Port**—Specify an operand (none, =, !, >, <) and a decimal value for the port number of the attack target.

- **Sequence Number**—Specify an operand (none, =, !, >, <) and a decimal value for the sequence number of the packet. This number identifies the location of the data in relation to the entire data sequence.

- **ACK Number**—Specify an operand (none, =, !, >, <) and a decimal value for the ACK number of the packet. This number identifies the next sequence number; the ACK flag must be set to activate this field.

- **Header Length**—Specify an operand (none, =, !, >, <) and a decimal value for the number of bytes in the TCP header.

- **Data Length**—Specify an operand (none, =, !, >, <) and a decimal value for the number of bytes in the data payload. For SYN, ACK, and FIN packets, this field should be empty.

- **Window Size**—Specify an operand (none, =, !, >, <) and a decimal value for the number of bytes in the TCP window size.

- **Urgent Pointer**—Specify an operand (none, =, !, >, <) and a decimal value for the urgent pointer. The value indicates that the data in the packet is urgent; the URG flag must be set to activate this field.

- **URG**—When set, the urgent flag indicates that the packet data is urgent.

- **ACK**—When set, the acknowledgment flag acknowledges receipt of a packet.

- **PSH**—When set, the push flag indicates that the receiver should push all data in the current sequence to the destination application (identified by the port number) without waiting for the remaining packets in the sequence.

- **RST**—When set, the reset flag resets the TCP connection, discarding all packets in an existing sequence.

- **SYN**—When set, the SYN flag indicates a request for a new session.
- FIN—When set, the final flag indicates that the packet transfer is complete and the connection can be closed.

- R1—This reserved bit (1 of 2) is not used.

- R2—This reserved bit (2 of 2) is not used.

**UDP Headers**

For attacks that use UDP and a packet context, in the Protocol tab, select **UDP Packet Header Fields** from TCP/UDP/ICMP Header Matches menu, then set values for the following UDP fields:

- Source Port—Specify an operand (none, = , !, >, <) and a decimal value for the port number on the attacking device.

- Destination Port—Specify an operand (none, = , !, >, <) and a decimal value for the port number of the attack target.

- Data Length—Specify an operand (none, = , !, >, <) and a decimal value for the number of bytes in the data payload.

**ICMP Headers**

For attacks that use ICMP and a packet context, in the Protocol tab, select **ICMP Packet Header Fields** from TCP/UDP/ICMP Header Matches menu, then set values for the following ICMP fields:

- ICMP Type—Specify an operand (none, = , !, >, <) and a decimal value for the primary code that identifies the function of the request/reply.

- ICMP Code—Specify an operand (none, = , !, >, <) and a decimal value for the secondary code that identifies the function of the request/reply within a given type.

- Sequence Number—Specify an operand (none, = , !, >, <) and a decimal value for the sequence number of the packet. This number identifies the location of the request/reply in relation to the entire sequence.

- ICMP ID—Specify an operand (none, = , !, >, <) and a decimal value for the identification number is a unique value used by the destination system to associate requests and replies.

- Data Length—Specify an operand (none, = , !, >, <) and a decimal value for the number of bytes in the data payload.
Configuring a Protocol Anomaly Attack Object

A protocol anomaly attack object locates unknown or sophisticated attacks that violate protocol specifications (RFCs and common RFC extensions). You cannot create new protocol anomalies, but you can configure a custom attack object that controls how the security device handles a predefined protocol anomaly when detected.

NOTE: Protocol Anomaly attack objects are supported by IDP-capable security devices only, such as the ISG 2000 or ISG 1000 running ScreenOS 5.0.0-IDP1.

To configure a custom protocol anomaly attack object, you must:

- Configure the false positive setting—For details, see “Configuring Attack Detection Properties” on page 248.
- Select a predefined protocol anomaly—Select the protocol anomaly you want to use for this attack object. The list of available predefined protocol anomalies depends on the protocols supported by the target platform. For details, refer to the NetScreen-Security Manager Online Help.
- Configure the time-based settings—For details, see “Configuring Time Binding” on page 248.

Configuring a Compound Attack Object

A compound attack object combines multiple signatures and/or protocol anomalies into a single attack object, forcing traffic to match all combined signatures and/or anomalies within the compound attack object before traffic is identified as an attack. By combining and even specifying the order in which signatures or anomalies must match, you can be very specific about the events that need to take place before the security device identifies traffic as an attack.

NSM 2006.1 and later releases also support Boolean expressions for standalone IDP signatures.

NOTE: Compound attack objects are supported by IDP-capable security devices only, such as the ISG series with Security Module or any of the standalone IDP Sensors. ISG series devices do not support Boolean expressions.

When configuring a custom compound attack object:

- All members of the compound attack object must use the same service setting or service binding, such as FTP, Telnet, YMSG, or TCP/80.
- You can add protocol anomaly attack objects to a compound attack object.
- You cannot add predefined or custom attack objects to a compound Attack Object. Instead, you specify the signature directly within the compound attack object, including such details as service (or service binding), service context, attack pattern, and direction.
You can add between 2 and 32 protocol anomaly attack objects and/or signatures as members of the compound attack object. However, all members must use the same service setting or service binding.

Configuring General Attack Properties
False positive and time-based attack properties are configured for a compound attack object the same way as they are for a signature attack object. For details, see “Configuring General Attack Properties” on page 245.

Because all members of the compound attack object must use the same service binding, the service binding you select determines the service contexts you can use for an attack pattern, as well as the available predefined protocol anomaly attack objects you can add as members.

To match all services, select **Any** as the Service Binding.

- When adding an attack pattern as a member, you are restricted to the contexts packet and first packet.
- When adding a predefined protocol anomaly attack object as a member, you are restricted to the IP-based protocol anomaly attack objects.

Additionally, because the number of session transactions are not known for the service, you cannot specify a scope (in the Members tab).

To match a specific service, select the service binding and provide the protocol ID, port/port range, program number if necessary.

Next, configure the members of the compound attack object.

Configuring Compound Attack Members
When configuring members, you add the signatures and/or protocol anomalies to detect an attack that uses multiple methods to exploit a vulnerability. The attack traffic must match all signatures and/or anomalies within the compound attack object before the device considers the traffic as an attack. To be explicit about the events in an attack, you can also specify the order in which signatures or anomalies must match before the security device identifies traffic as an attack.

Configuring Attack Object Scope
If the selected service supports multiple transactions within a single session, you can also specify whether the match should occur over a single session or can be made across multiple transactions within a session:

- Select **Session** to allow multiple matches for the object within the same session.
- Select **Transaction** to match the object across multiple transactions that occur within the same session.
Configuring An Attack Pattern
You configure the attack pattern as a member of a compound attack object as you would an attack pattern in a signature attack object. For details, see “Configuring Attack Detection Properties” on page 248.

To add an attack pattern to the compound Attack Object, click the Add icon and select Signature.

- Pattern—Specify the pattern to match. You construct the attack pattern just as you would when creating a new signature Attack Object. To negate the pattern, enable Negate.
- Context—Specify the context in which to locate the pattern. The context displays only contexts that are appropriate for the specified Service. If you selected a service binding of Any, you are restricted to the service contexts packet and first packet.
- Direction—Specify whether the security device should match the pattern in traffic flowing in any direction, from client to server, or from server to client.

Adding A Predefined Protocol Anomaly Attack Object
To add a protocol anomaly to the compound attack object, click the Add icon and select protocol anomaly. In the Attack Properties area, select an anomaly from the Key menu. The menu only displays protocol anomalies appropriate for the Service you selected.

If you selected a service binding of any, you are restricted to the IP-based protocol anomaly attack objects.

Configuring Attack Object Ordered Match
Use ordered match to create a compound Attack Object that must match each member signature or protocol anomaly in the order you specify. If you do not specify an ordered match, the compound Attack Object still must match all members, but the attack pattern or protocol anomalies can appear in the attack in random order.

To configure an ordered match, enable Ordered Match and use the arrow keys to reorder members.

Or, use the Boolean Expression field match a more complex arrangement of attack patterns.

Configuring Boolean Expression
Using the Boolean Expression field disables the Ordered Match function for standalone IDP devices. For ISG devices, the Boolean Expression field is ignored and the Ordered Match checkbox is used, if it is checked.

The Boolean Expression field makes use of the Member Names created in the lower part of the dialog.

NSM supports three Boolean operators: or, and, and oand (ordered and). NSM also supports the use of parenthesis to determine precedence.
Boolean operators:

- or - if either of the member name patterns match, the expression matches.
- and - if both of the member name patterns match, the expression matches. It does not matter which order the members appear in.
- oand - if both of the member name patterns match, and if they appear in the same order as in the Boolean Expression, the expression matches.

EXAMPLE: BOOLEAN EXPRESSION
Suppose you have created six signature members, labelled s1 - s5.

Suppose you know that the attack always contains the pattern s1, followed by either s2 or s3. Further, you know that the attack always contains s4 and s5, but their positions in the attack can vary.

You might create the following Boolean expression:

\[((s1 oand s2) or (s1 oand s3)) and (s4 and s5)\]

Configuring Direction Filter

Use the direction filter to specify the direction (Any, Client-to-Server, Server-to-Client) of traffic in which the attack object attempts to match an attack. Each attack version in the attack object retains its own direction; however, you can use the direction filter to change which direction is monitored by the attack object. Only those attack versions that match the direction filter are active in the attack object.

By default, the direction filter is automatically set to the direction of the most recently-created or edited attack version.

Creating Custom DI Attack Groups

You can create custom attack object groups to contain your custom DI attack objects. After you add these custom groups to a DI profile, you can then configure a firewall rule to use that DI Profile.

All DI attack object groups (both predefined and custom) are considered “static” groups, meaning that they do not change. To add or delete an attack object from the group, you must manually edit the group members.

A custom attack object group can contain custom attack objects and other custom attack object groups. You cannot add predefined attack objects or predefined attack object groups to a custom attack object group. To use both predefined and custom attack objects in a firewall rule, create a DI Profile that includes predefined and custom attack object groups, then use this profile object within the Rule Options of a firewall rule. For information about creating a DI Profile, see “Creating DI Profiles” on page 235.

NOTE: Attack group names cannot be the same as attack object names.
Creating Custom IDP Attack Groups

NetScreen-Security Manager contains a database of hundreds of predefined attack objects designed to protect networks from multiple attack vectors.

For IDP attack objects, you can create static or dynamic groups to contain predefined or custom attack objects. A static group contains only the groups or attack objects you specify, while a dynamic group contains attack objects based on criteria you specify. Although you do not have to create a group to use an attack object within an IDP rule (you can add attack objects individually or by group), organizing attack objects into groups can help keep your Security Policies organized.

Creating Static Attack Groups

A static group contains a specific, finite set of attack objects or groups. There are two types of static groups: predefined static groups and custom static groups.

A custom static group can include the same members as a predefined static group (predefined attack objects, predefined static groups, and predefined dynamic groups), plus the following members:

- Custom attack objects
- Custom dynamic groups
- Other custom static groups

Use static groups to define a specific set of attacks to which you know your network is vulnerable, or to group custom attack objects. For example, you might want to create a group for a specific set of informational attack objects that keep you aware of what is happening on your network.

Static groups require more maintenance than dynamic groups because you must manually add or remove attack objects in a static group to change the members. However, you can include a dynamic group within a static group to automatically update some attack objects. For example, the predefined attack object group Operating System is a static group that contains four predefined static groups: BSD, Linux, Solaris, and Windows. The BSD group contains the predefined dynamic group BSD-Services-Critical, to which attack objects can be added during an attack database update.

To create a custom static group:

1. In Object Manager, select Attack Objects > IDP Objects. The IDP Objects dialog box appears.
2. Click the Custom Attack Groups tab, then click the Add icon and select Add Static Group. The New Static Group dialog box appears.
3. Enter a name and description for the static group. Select a color for the group icon.
4. To add an attack or group to the static group, select the attack or group from the Attacks/Group list and click the Add button.
5. Click OK.

For instructions for creating a static attack object group, see the NetScreen-Security Manager Online Help topic “Adding Static Attack Groups”.

Creating Dynamic Attack Groups (IDP Only)

A dynamic group contains a dynamic set of attack objects that are automatically added or deleted based on specified criteria for the group. For example, an attack database update can add or remove attack objects from a dynamic group based on the group criteria. This eliminates the need to review each new signature to determine if you need to use it in your existing Security Policy.

A predefined or custom dynamic group can only contain attack objects and not attack groups. Dynamic group members can be either predefined or custom attack objects.

To create a custom dynamic group:

1. In Object Manager, select **Attack Objects > IDP Objects**. The IDP Objects dialog box appears.

2. Click the Custom Attack Groups tab, then click the Add icon and select **Add Dynamic Group**. The New Dynamic Group dialog box appears.

3. Enter a name and description for the static group. Select a color for the group icon.

4. In the Filters tab, click the Add icon and select one of the following:

   - **Add Products Filter** to add attack objects based on the application that is vulnerable to the attack.
   - **Add Severity Filter** to add attack objects based on the attack severity.
   - **Add Category Filter** to add attack objects based on category.
   - **Add Last Modified Filter** to add attack objects based on their last modification date.
   - **Add Recommended Filter** to include only attacks designated to be the most serious threats to the dynamic group. In the future, Juniper Networks will designate only attacks it considers to be serious threats as Recommended. These settings will be updated with new attack object updates. In addition, you can designate custom attack objects as Recommended or not.

   **NOTE:** All predefined attack objects are assigned a severity level by Juniper Networks. However, you can edit this setting to match the needs of your network.

   - **Add Category Filter** to add attack objects based on category.
   - **Add Last Modified Filter** to add attack objects based on their last modification date.
   - **Add Recommended Filter** to include only attacks designated to be the most serious threats to the dynamic group. In the future, Juniper Networks will designate only attacks it considers to be serious threats as Recommended. These settings will be updated with new attack object updates. In addition, you can designate custom attack objects as Recommended or not.

   You create filters one at a time; each criteria you add is compared to the attributes for each attack object. Attack objects that do not match the criteria are immediately filtered out. If you create a filter with attributes that no attack object can match, a message appears warning you that your dynamic group has no members.
From the resulting list of matching attack objects, you can then exclude any attack objects that produces false positives on your network, or an attack object that detects an attack to which your network is not vulnerable.

NOTE: A dynamic group cannot contain another group, (predefined, static, or dynamic). However, you can include a dynamic group as a member of a static group.

EXAMPLE: CREATING A DYNAMIC GROUP
To create a dynamic group:

1. In the Custom Attack Groups tab, click the Add icon and select Add Dynamic Group. The New Dynamic Group dialog box appears.

2. Enter a name and description for the group. Select a color for the group icon.

3. In the Filters tab, click the Add icon and add the filters that determine which attack objects should be in the group:
   a. Add a Products filter to add attack objects that detect attacks against all Microsoft Windows operating systems.
   b. Add a Severity filter to add attack objects that have a severity level of critical or major.

IDP automatically applies all filters to the entire attack object database, identifies the attack objects that meet the defined criteria, and adds the matching objects as members of the group.

4. View the members of the group by clicking the Members tab:
5. Click OK to save the dynamic group.

**Updating Dynamic Groups**

When you are satisfied with the group criteria and its members, use the group in a Security Policy. The next time you update your attack objects, the update automatically performs the following:

- For all new attack objects, compares the predefined attributes of each attack object to each dynamic group criteria and adds the attack objects that match.

- For all updated attack objects, removes attack objects that no longer meet their dynamic group criteria. The update also reviews updated attack objects to determine if they now meet any other dynamic group criteria, and adds them to those groups if necessary.

- For all deleted attack objects, removes the attack objects from their dynamic groups.

You can also edit a dynamic group manually, adding new filters or adjusting existing filters to get exactly the type of attack objects your want.

**NOTE:** You can edit a custom dynamic attack group from within an IDP rule in a Security Policy. Double-click the group icon in the Attack Objects column of an IDP rule to display the Dynamic Group dialog box, make the desired changes, then click OK to save your edits.
Editing a Custom Attack Group

To modify a custom attack group, double-click the group in the Custom Attack Groups tab in the IDP Objects dialog box. The Static Group or Dynamic Group dialog box appears, with the previously-configured information displayed. Enter any changes you want to make and then click Apply to continue making changes or click OK to close the dialog box.

Deleting a Custom Attack Group

To delete a custom attack group, right-click the group in the Custom Attack Groups tab in the IDP Objects dialog box, and then select Delete. A confirmation window asks you to verify that you want to delete the item. Click OK.

Configuring Custom Policy Fields

Custom Policy Fields objects represent metadata information that you can store and use in a structured manner. Users can add custom objects to the policy table, such as ticket Number, vendor contact, and so on, for each rule in the rulebase. NSM provides a shared object to store these custom detail data while the table contains a column that corresponds to these custom details.

The Custom Detail column (visible only in Expanded Mode and hidden in Compact Mode) captures the information about the rule, but does not push the information to the device. The column is able to display multiple shared objects in each cell.

This allows for a better filtering mechanism for the information, reduces data redundancy (in the case where all rules need to have the same email address associated with them), and provides multiple properties for user’s needs.

The Custom Detail Object is user configurable. The metadata is designed to capture the following information about each object:

- **Name** – Determines to which definition of the metadata the objects need to comply.

- **Required** – Indicates if the metadata for a Custom Detailed Object is defined with the “Required” option set to true, all rules in all rulebases that do not have a value selected for this MetaData displays the yellow warning triangle with a warning message. The policy will not be saved if no value is provided.

- **Validation String** – A Shard Object definition in the metadata requires the user to select from a list of Custom Detail objects. A String definition in the metadata allows the user to enter a plain test string. Each instance supports no more than a single string value.

- **Field Type** – If a regular expression is provided in the definition of an object, the custom detail object is validated against the regular expression. This is required and the Custom Object instance cannot be saved until this expression is satisfied.

- **Comments** – This column allows the user to input any comments associated with the new object.
Defining Metadata

The metadata is defined using the Policy Details node located in the navigation tree. Users can see all metadata definitions as well as add, edit, or delete definitions. Existing metadata is displayed in table format and supported at the domain level. Definitions in the global domain are accessible in sub-domains for creating objects that comply with the global domain.

Deleting a metadata definition forces all objects to comply with the definition and lists all usages of those objects. When deleting a metadata definition, all the objects complying that metadata are also deleted. In addition, it removes all usages of the changed objects from the security policy rules that referred to them.

Instantiating New Objects

As with metadata definitions, you can also create custom policy objection on the domain level. Objects you create in the global domain will be available for all sub-domains, while objects created in the sub-domains will only be available within the sub-domain in which it was created.

When you delete an object, NSM displays all the usages of that object in the security policy rules, and will ask you for confirmation of the command. Once you confirm that you want to delete the object, NSM will remove all usages of the object you are deleting from the security policy rules that refer to the deleted object.

Adding Custom Detail Object to Rules

You can add custom detail objects to a rule in the policy using the same mechanism as other shared objects, such as Service or Address Objects. You can use multiple selections for objects using the Shared data type. This allows you to add multiple objects complying with the same metadata. For example, you can add multiple email addresses or phone number for each rule.

Once you have added custom objects to the rules, NSM displays the custom object along with the metadata name. For example, after adding an address to a rule, the value displayed in the rule could look like the following:

Email Address: admin@juniper.net
Requisition Number: JN0001

NSM will sort the entries in the Custom Details cell by the metadata name appended to the custom object value. NSM will be copy and paste data in the Custom Details column along with other rule data when a rule is copied and pasted.

Objects with a String data type will provide a special edit dialog that allow you to change the string value contained within. The dialog allowing for this information is accessible by right-clicking on the selected value in the Context Menu. Objects with a Shared data type will have a special dialog that allows you to edit the value contained within. After saving the change, it is reflected in all rules using that object.
Configuring AntiVirus Objects

Security devices provide one or more of the following antivirus scanning methods:

- External AV scanning—This method forwards traffic to a Trend Micro device for scanning. (This option is not supported by devices running ScreenOS 5.1 or higher.) The security device forwards all traffic to be scanned to the Trend Micro device. To configure external AV scanning, use the AV Scanner settings (detailed below).

- Internal AV scanning—This method uses the AV scanner on the security device, and is not supported by all security devices. Internal scanning may be configured on a per-device basis, or it may be configured via templates. This section describes how to create the templates.

- ICAP AV scanning—This method forwards traffic to an Internet Content Adaptation Protocol (ICAP) server for examination. To forward traffic to an ICAP server, create an ICAP server object, create an ICAP profile, and then specify that profile in a policy.

Configuring External AV Profiles

External AV profiles define the external Trend Micro AV scanner server that a security device uses to detect viruses in specific protocols. This feature describes the external scanner supported by ScreenOS 5.0. For ScreenOS 5.4 and later, use an ICAP AV profile as described in Configuring ICAP AV Servers and Profiles on page 268.

You must configure an AV profile when using external AV for virus protection on your security device. After you have configured an AV profile, you can use the profile within a firewall rule.

NOTE: You can configure additional settings for external antivirus protection on the security device itself. For details, see “NetScreen-Security Manager: Configuring Firewall/VPN Devices”.

External AV profiles contain the following information:

- Server Name and Port—You must specify the IP address and port number of the external antivirus server that contains your virus definitions.

- Protocols and Timeouts—You must specify the protocols (HTTP and/or SMTP) that the external AV server scans for viruses. The default protocol timeout is 180 seconds, but you can edit this default to meet your networking requirements.
You must use the AV profile in a firewall rule and install that rule on a security device before the external scanner can begin inspecting traffic for viruses. For information about using AV profiles in rules, see “Configuring AntiVirus For Firewall Rules” on page 344.

EXAMPLE: CONFIGURING AN EXTERNAL AV PROFILE
In this example, you configure an AV profile that sends all HTTP traffic to an external antivirus server at 1.2.2.20 for virus checking. Because you anticipate heavy HTTP loads on the network, you increase the timeout from 180 seconds (the default setting) to 300 seconds.

1. In the main navigation tree, select Object Manager > AV Objects > External.

2. In the main display area, click the Add icon. The New AntiVirus Profile dialog box appears.

3. Configure the following:
   - For Name, scanner1_HTTP
   - For Server Name, enter 1.2.2.20.
   - For Server Port, leave the default port number of 3300.

4. Select HTTP, then configure the timeout as 300 seconds.

5. Click OK to save the new profile.

Configuring Internal AV Profiles
Internal AV profiles allow you to set AV settings for multiple devices via a policy. NetScreen-Security Manager comes with a predefined AV profile, or you can create your own.

View the Predefined Profile
To view the predefined AV profile, open Object Manager > AV Objects > Internal > Predefined Profiles. Select the predefined profile, then click the edit button. You cannot make changes to the profile.

Create Custom AV Profiles
To create a custom AV profile, open Object Manager > AV Objects > Internal > Custom Profiles. Click the Add button.

Populate the fields of the New Internal Antivirus Profile dialog:
- General information—Assign a name and color to the profile, and enter a comment describing the purpose of the profile.
- For each protocol type, check the Enable checkbox to enable scanning for that protocol, then set the following settings for each enabled protocol:
  - Scan Mode: All, Intelligent, or by File Extension. If you select Scan by File Extension, you must populate the Ext List Include field.
Configuring AntiVirus Objects

Chapter 8: Configuring Objects

- Scanning Timeout: scans that take longer than this time out and are not completed.

- Decompress Layer: the number of levels of decompression to uncompress before scanning. A decompression setting of 2 would uncompress all the scanning of a .zip file within a .zip file.

- Skip Mime (HTTP only): if checked, causes the scanner to skip any mime types listed in the Mime List field.

- Ext List Include: a list of file extensions to examine for viruses. Extension lists are created under Object Manager > AV Objects > Extension Lists.

- Ext List Exclude: a list of file extensions to not examine for viruses. Extension lists are created under Object Manager > AV Objects > Extension Lists.

- Mime List (HTTP only): the list of mime types to not scan. NetScreen-Security Manager ships with a default mime type list, or you can create your own under Object Manager > AV Objects > Custom Mime Lists.

- Email Notify Virus Sender (IMAP, POP3, SMTP only): Notifies an email sender if a virus was found in the email.

- Email Notify Scan-Error Sender (IMAP, POP3, SMTP only): Notifies an email sender if the email was dropped due to a scan error.

- Email Notify Scan-Error Recipient (IMAP, POP3, SMTP only): Notifies an email recipient if the email was passed due to a scan error.

Configuring Extension Lists

You can configure AV profiles to scan (or not scan) files based on their file extension. File extension include lists and exclude lists are the same kind of lists. They become include or exclude lists depending on how they are added to a profile.

To create a file extension list object, open Object Manager > AV Objects > Internal > Extension lists. Click Add.

Populate the following fields in the New Internal Antivirus Ext List dialog:

- Name: Give the extension list a descriptive name.

- Color: Assign a color, if desired.

- Comment: Provide a comment describing the list and its use.

- File Extension: enter a list of file extensions, separated by semicolons. Example: html;htm;jpg.
Configuring Mime Lists

You can tell your device to skip certain mime types when scanning HTTP streams. Do this by checking the Skip Mime checkbox in the profile dialog, then specifying a mime list.

Mime lists are used by Internal and ICAP AV Profiles.

To create a mime list, open Object Manager > AV Objects > Custom Mime lists. Click Add.

Populate the following fields in the New Internal Antivirus Mime List dialog:

- **Name**: Give the mime list a descriptive name.
- **Color**: Assign a color, if desired.
- **Comment**: Provide a comment describing the list and its use.
- **File Extension**: enter a list of mime types, separated by semicolons. Example: application/postscript;text/html;image/bmp.

NetScreen-Security Manager comes with Predefined Mime lists. To view them, open Object Manager > AV Objects > Predefined Mime lists.

Configuring ICAP AV Servers and Profiles

Through NSM, you can configure security devices to forward traffic to an ICAP AV server or server group. If you specify a group of servers, the security device load balances between the servers based on parameters you specify.


Configuring ICAP AV Servers and Server Groups

Before a security device can forward traffic to an ICAP AV server, you must create a server object in NSM. You can create multiple server objects and assign some or all of them to server groups. You can then assign this server object or server group to an AV profile, then assign that profile to a security policy.

To specify an ICAP server in NSM, select Object Manager > ICAP > Servers and Server Groups. Click the + button to either specify a new server, or to create a new group and assign servers to it. You cannot assign server groups to server groups.

To specify a server, you will need the following information:

- **Name**: The name of the ICAP server as it will appear in the NSM GUI.
- **Host**: The IP address of the ICAP server.
- **Port**: The ICAP server port. (Default: 1143)
- **Enable**: If selected, indicates that the server should be reachable and usable by a security device. Unselect this checkbox if the server is unavailable or should not be used by a security device.
- **Probe URL**: The path on the ICAP AV server to probe for availability.

- **Probe Interval (in seconds and multiples of 5)**: Indicates how often the security device should check to see that the server is in service and available to process traffic. If this value is set to 0, then the security device will assume that the ICAP service is available at all times. If it is set to a positive number of seconds, the security device will check the server’s status at that interval. If the server returns as in-service, the security device will send it traffic. If it returns as out-of-service, the security device will not send traffic.

- **Maximum Connections**: The maximum number of TCP connections between the security device and the ICAP AV server.

To create a server group, first create the server objects that will go into it. However, you can create an empty group as a place holder.

You can assign a server to more than one server group.

### Configuring ICAP AV Profiles

ICAP AV profiles, when assigned to a policy, redirect traffic to an ICAP AV server.

To create an ICAP AV Profile, select **Object Manager > AV Objects > ICAP > Custom Profiles**. Then, click the **+** button.

You need the following information:

- **General information**—Assign a name and color to the profile, and enter a comment describing the purpose of the profile.

- **HTTP tab**:
  - **HTTP Enable**: Selecting this checkbox in each tab turns on scanning for that protocol.
  - **Skip Mime**: If checked, causes the scanner to skip any mime types listed in the Mime List field.
  - **Time out**: Scans that take longer than this time out and are not completed.
  - **Mime List**: If Skip Mime is checked, also specify the MIME list that will be used for comparison. See Configuring Mime Lists on page 268 for information on creating MIME lists.

- **SMTP tab**:
  - **SMTP Enable**: Selecting this checkbox in each tab turns on scanning for that protocol.
  - **Time out**: Scans that take longer than this time out and are not completed.
  - **Email Notification for Virus - Notify Sender**: Notifies an email sender if a virus was found in the email.
Email Notification for Scan - Notify Sender: Notifies an email sender if the email was dropped due to a scan error.

Email Notification for Scan - Notify Recipient: Notifies an email recipient if the email was passed due to a scan error.

ICAP tab:

ICAP Server/Server Group: Assign an ICAP AV server or server group to this profile. See Configuring ICAP AV Servers and Server Groups on page 268 for information on creating ICAP AV servers and server group objects in NSM.

Request URL: The request URL on the ICAP AV server.

Response URL: The response URL on the ICAP AV server.

Configuring Web Filtering Objects

Web Filtering (Integrated) enables you to create a Web Filtering profile for all of your security devices by binding the profile to the firewall rule. With a Web Filtering profile, the security device intercepts each HTTP request and determines whether to permit or block access to a requested website by categorizing the URL and matching the Web category to the Web Filtering profile. You can then bind the Web Filtering profile to the firewall rule.

To configure a security device for Web Filtering, you need to:

- Obtain a license key to enable the Web Filtering option on security devices. For details, see “Managing License Keys” on page 196.
- Configure at least one Domain Name Server (DNS) so the security device can resolve the SurfControl CPA server name to an address.
- Configure Web Filtering on the security device. For details, see “NetScreen-Security Manager: Configuring Firewall/VPN Devices”. 
Web Categories

A Web category is a list of URLs organized by content. There are two types of categories: Custom Lists and Predefined Categories.

Custom Lists

You can group URLs and create custom lists specific to your needs. You can include up to 20 URLs in each list. When you create a list, you can add either the URL or the IP address of a website. When you add a URL to a custom list, the security device performs a Domain Name Server (DNS) lookup, resolves the hostname into IP addresses and caches this information.

When a user tries to access a website by typing the IP address of the website, the security device checks the cached list of addresses and tries to resolve the hostname. It is important to enter both the URL and the IP address(es) of a website.

NOTE: When a URL exists in both a custom list and a predefined category, the security device matches the URL to the custom list first.

EXAMPLE: CREATING A URL CUSTOM LIST

In this example you create a custom list called Competitors, Gaming.

1. In the main navigation tree, select Object Manager > Web Filtering (Integrated) > Web categories > Custom Lists.

2. Click the Add icon. The New Web categories dialog box appears.

3. For Name, enter Competitors, Gaming.

4. Click the Add icon. The New URL Entries dialog box appears. Configure as shown in Figure 59, then repeat to add a second URL Entry.
Figure 59: Create New Custom URL List

For the first URL entry, enter www.games1.com then click OK.

For the second URL entry, enter www.games2.com then click OK.

5. Click OK to save the new Custom List.

Predefined Categories

The security devices can use the predefined SurfControl Web categories to determine the category of a URL. SurfControl Content Portal Authority (CPA) servers maintain a large database of web content classified into approximately 40 categories.

To view the predefined SurfControl Web categories, select Web Filtering (Integrated) > Web categories > Predefined Categories.
Web Profiles

A Web Filtering profile consists of a group of Web categories and their corresponding actions. NetScreen-Security Manager supports two types of profiles: Custom and Predefined.

Custom Profiles
When you create a custom Web Filtering profile, you can add both custom and SurfControl predefined Web categories to the profile, then specify a category for the Black List and/or the White List.

- Black List—The security device always blocks access to the web sites in the Black List. You can create a custom category for the Black List or use a predefined category.

- White List—The security device always allows access to the web sites in the White List. You can create a custom category for the White List or use a predefined category.

You can also configure the default action for the profile:

- Permit—The security device allows access to the website.

- Block—The security device does not allow access to the website. When the device blocks access to a website, it displays a message indicating the category of the URL.

EXAMPLE: CREATING A WEB FILTERING CUSTOM PROFILE
In this example, you create a custom profile called Competitors.

1. From the main navigation tree, select Object Manager > Web Filtering (Integrated) > Web Profiles > Custom Profiles.

2. Click the Add icon. The New Web Profile dialog box appears. Configure the following, then click OK:

   - For Name, enter Competitors.

   - For Comments, enter All Competitors.

   - For Black List, select Competitors, Gaming.

   - For White List, select None.

3. In Main Categories, click the Add icon and select the following Web categories: Art and Entertainment, Games. Click OK to add to the profile object.

4. Select Games, then click the Edit icon. Change the default action for the Games category to Block, then click OK, as shown in Figure 60.
Configuring Web Filtering Objects

5. For **Action for all Other URLs**, leave the default setting (Block).

6. Click **OK** to save the new Profile.

Predefined Profiles

NetScreen-Security Manager provides a default profile called **ns-profile**. It lists the SurfControl predefined Web categories and their corresponding actions.

**NOTE:** If the URL in an HTTP request is not listed in a custom profile, then the security device defaults to ns-profile.

**NOTE:** You cannot edit the default profile or add a Black List or White List to it.

**EXAMPLE:** VIEWING THE PREDEFINED PROFILE

To view the predefined profile:

1. **In the main navigation tree, select Object Manager > Web Filtering (Integrated) > Web Profiles > Predefined Profiles.**

2. **Double-click ns-profile.** The Web Profile dialog box displays the Categories and Actions for the ns-profile.

**NOTE:** You cannot change the list of predefined categories in ns-profile.
Configuring GTP Objects

To enable a security device to manage GTP traffic, you must create a GTP Object and then apply it to a Security Policy rule. The rule with the GTP object defines how the device handles GTP packets: If a GTP packet matches the rule, the device attempts to further match the packet data with the parameters set in the GTP object.

For detailed information on GTP, refer to the ScreenOS Concepts and Examples Guide, Volume 13: General Packet Radio Service.

Using GTP objects, you can configure multiple rules that enforce different GTP configurations in the same Security Policy. For example, you can configure a Security Policy that enables a device to control GTP traffic differently based on source and destination zones and addresses, action, and so on.

You configure GTP Objects in the Object Manager. From the main navigation tree, select Object Manager > GTP Objects, then click the Add icon to display the New GTP Object configuration screens. For each object, you can configure the following settings:

- Configuring Info
- Configuring Traffic Logging and Counting
- Configuring IMSI Prefix and APN Filtering
- Configuring GTP Message Filtering
- Configuring Subscriber Tracing (Lawful Interception)

The following sections detail each GTP setting. For an example on creating a GTP object, see “Creating a GTP Object” on page 280.

Configuring Info

The Info settings define the basic properties of the GTP object, and specify how the security device should handle GTP messages and tunnels.

Limiting GTP Message Length

To limit the length of a GTP message, you can specify the minimum and maximum number of bytes permitted in a message length field. In the GTP header, the message length field indicates the length of the GTP payload. It does not include the length of the GTP header itself, the UDP header, or the IP header.

The default minimum and maximum GTP message lengths are 0 and 65535, respectively.

Limiting GTP Message Rate

To limit the rate of network traffic from a security device to a GPRS Support Node (GSN), you can specify the number of packets per second permitted for GTP-Control (GTP-C) messages.
Because GTP-C messages require processing and replying, they can overwhelm a GSN. Setting a rate limit on GTP-C messages can protect your GSNs from Denial-of-Service (DoS) attacks such as:

- **Border Gateway bandwidth saturation**—A malicious operator connected to the same GRX as your PLMN can generate enough network traffic directed at your Border Gateway, so that legitimate traffic is starved for bandwidth in or out of your PLMN, thus denying roaming access to or from your network.

- **GTP flood**—GTP traffic can flood a GSN, forcing it to spend its CPU cycles processing illegitimate data. This can prevent subscribers from roaming, forwarding data to external networks, or prevent a GPRS attach to the network.

To limit the GTP message rate, enable Limit (packets/second) and enter the maximum number of packets per second that a security device can send to a GSN (the default is unlimited).

**Limiting GTP Tunnels**

GSNs use GTP tunnels to transmit GTP traffic using the GPRS Tunneling Protocol (GTP). Because GSNs have a limited capacity for GTP tunnels, you might want to configure the security device to limit the number of GTP tunnels created.

To limit GTP tunnels, enable Limit (tunnels/GSN) and enter the maximum number of tunnels permitted for each GSN (the default is unlimited).

**Removing Inactive GTP Tunnels**

To configure a security device to detect and remove inactive GTP tunnels automatically, configure the GTP Tunnel Inactivity Timeout (hours). A GTP tunnel might hang (become inactive) when a “delete pdp context response” message gets lost on a network, or a GSN does not properly shut down.

The security device automatically removes a GTP tunnel that is idle for the specified timeout value. The default timeout value is 24 hours.

**Validating Sequence Numbers**

When using a security device between the GGSNs, you can configure the device to validate sequence numbers for the GGSN and drop out-of-sequence packets. This helps conserve GGSN resources by preventing the unnecessary processing of invalid packets.

The header of a GTP packet contains a Sequence Number field, which indicates the order of the packets arriving at the GGSN. During the PDP context activation stage:

- The sending GGSN uses zero (0) as the Sequence Number value for the first G-PDU it sends through a tunnel to another GGSN. The sending GGSN then increments the Sequence Number value for each following G-PDU it sends. The value resets to zero when it reaches 65535.
The receiving GGSN sets its counter to zero. When it receives a valid G-PDU, it increments its counter by one. The counter resets to zero when it reaches 65535. The receiving GGSN compares the Sequence Number in the arriving packet with the sequence number in its counter: If the numbers correspond, the GGSN forwards the packet; if they differ, the GGSN drops the packet.

To enable the device to validate sequence numbers for the GGSN, enable Sequence Number Validation. By default, validation is disabled.

Filtering GTP-in-GTP Packets
To enable a security device to detect and drop a GTP packet that contains another GTP packet in its message body, enable GTP in GTP Denied.

Removing GTP R6 Informational Elements
GTP R6 contains additional Informational Elements (IEs) that support 3GPP networks: RAT, RAI, ULI, IMEI-SV, and APN Restriction. These new IEs are not supported on 2GPP networks. You can tell the firewall to strip out these elements when traffic passes from a 3GPP network to a 2GPP network.

To enable GTP traffic to flow between 3GPP and 2GPP networks, enable Remove r6 IE.

Inspecting Tunnel Endpoint IDs
You can configure the security device to perform Deep Inspection on the tunnel endpoint IDs (TEID) in G-PDU data messages.

To perform Deep Inspection on tunnel endpoint IDs, enable TEID DI.

Configuring Traffic Logging and Counting
When you enable traffic logging and counting for a GTP object, the security device generates log entries for deleted GTP tunnels and GTP traffic events.

Traffic Counting
A security device can count the number of user data and control messages (or bytes of data), received from and forwarded to the GGSNs and SGSNs that the device protects. The device counts traffic for each GTP tunnel separately, and differentiates GTP-User and GTP-Control messages.

To enable counting, select Count By Message or Count By Byte. When counting is enabled and tunnel is deleted, the device counts and logs the total number of messages or bytes of data that it received from and forwarded to the SGSN or GGSN.

To view log entries for deleted GTP tunnels, use the Log Viewer. For information about the information provided in the GTP log entry, see “GTP Log Entries” on page 776.
Traffic Logging

A security device creates log entries for GTP events based on the status of the GTP packet. For each event type, you can also specify how much information (basic or extended) you want about each packet (for details, see “GTP Log Entries” on page 776).

To configure GTP logging, select basic or extended for each GTP packet status:

- Log Forwarded Packets—When enabled, the device creates a log entry for each GTP packet that was transmitted because it was permitted by the Security Policy.
- Log Dropped Packet Due to Type/Length/Version—When enabled, the device creates a log entry for each GTP packet that was dropped because it was denied by the Security Policy.
- Log Dropped Packet Due to Invalid State—When enabled, the device creates a log entry for each GTP packet that was dropped because it failed stateful inspection.
- Log Dropped Packet Due to GSN Tunnel Limit—When enabled, the device creates a log entry for each GTP packet that was dropped because the maximum limit of GTP tunnels for the destination GSN was reached.
- Log Dropped Packet Due to GSN Rate Limit—When enabled, the device creates a log entry for each GTP packet that was dropped because the maximum rate limit of the destination GSN was reached.

You can also specify the frequency that a security device creates log entries for rate-limited messages. Setting a logging frequency conserves resources on the syslog server and security device, and can avoid a logging overflow of messages. By default, the frequency is 2, meaning the security device creates a log entry for every two messages above the set rate limit.

To view GTP traffic log entries, use the Log Viewer.

Configuring IMSI Prefix and APN Filtering

You can use the IMSI Prefix and APN to restrict access to a specific set of mobile subscribers.

Creating an APN Filter

An Access Point Name (APN) is included in the header of a GTP packet, and provides information on how to reach a network. By default, a security device permits all APNs. However, you can configure the device to filter APNs, enabling access only for those APNs you specify, and restricting roaming subscribers’ access to external networks.

You can specify up to 2000 permitted APNs. When APN filtering is enabled, it applies only to “create pdp request” messages. For these messages to pass an APN filter, the GTP packet must match both the APN name filter and the Selection Mode filter:
- APN Domain Name filter—The device attempts to match the APN in a GTP packet to the APNs set in the GTP object. If the two APNs match, the device passes the packet to the selection mode filter.

- Selection Mode Filter—The device attempts to match the Selection Mode for the GTP packet and the GTP object. If the two modes match, the device forwards the GTP packet; if the modes do not match, the device drops the GTP packet.

Additionally, you can filter GTP packets based on the combination of an IMSI prefix and an APN. For details, see “Creating an IMSI Prefix Filter” on page 279.

**Setting the Network ID (APN Domain Name)**
To set an APN filter, you need to know the network ID, which identifies the name of an external network.

---

**NOTE:** Because the APN domain name (network ID) can potentially be very long and contain many characters, you can use the wildcard “*” as the first character of the APN to indicate that the APN also includes all preceding characters. However, because APN filtering is based on perfect matches, using the wildcard “*” can prevent the inadvertent exclusion of APNs that you would otherwise authorize.

---

**Setting a Selection Mode**
You must also set a Selection Mode, which indicates the origin of the APN and if the user subscription has been verified by the Home Location Register (HLR). You can set one of the following Selection Modes:

- Mobile Station—MS-provided APN, subscription not verified. This Selection Mode indicates that the mobile station (MS) provided the APN and that the HLR did not verify the user’s subscription to the network.

- Network—Network-provided APN, subscription not verified. This Selection Mode indicates that the network provided a default APN because the MS did not specify one, and that the HLR did not verify the user’s subscription to the network.

- Verified—MS or Network-provided APN, subscription verified. This Selection Mode indicates that the MS or the network provided the APN and that the HLR verified the user’s subscription to the network.

**Creating an IMSI Prefix Filter**
A GSN (GPRS Support Node) identifies a mobile station by its IMSI (International Mobile Station Identity). An IMSI is composed of three elements:

- The MCC (Mobile Country Code)
- The MNC (Mobile Network Code)
- The MSIN (Mobile Subscriber Identification Number)
The MCC and MNC combine to create the IMSI prefix, which identifies the mobile subscriber’s home network (PLMN). By default, a security device does not perform IMSI prefix filtering on GTP packets. You can use the IMSI prefix to configure a security device to deny GTP traffic sent from non-roaming partners.

When you set an IMSI prefix in the GTP object, the security device filters “create pdp request” messages and permits only GTP packets with a matching IMSI prefix. If the prefix does not match, the security device drops the GTP packet. You can set up to 1000 IMSI prefixes for each device (one per each filter).

To disable IMSI prefix filtering, remove all MCC-MNC pairs from the GTP object.

**Configuring GTP Message Filtering**

By default, the security device permits all GTP message types. You can configure a security device to filter GTP packets and drop them based on their message type.

A GTP message type includes one or many messages. When you drop a message type, you automatically drop all messages of the specified type. For example, if you select to drop the `sgsn-context` message type, you also drop “sgsn context request”, “sgsn context response”, and “sgsn context acknowledge” messages.

You drop message types based on the GTP version number, enabling you to drop message types for one version and permit them for another version.

**Configuring Subscriber Tracing (Lawful Interception)**

You can configure a security device to identify subscribers based on IMSI prefixes or Mobile Station-Integrated Services Data Network (MS-ISDN) identification, then log the contents of their GTP-User Data (GTP-U) or GTP-Control (GTP-C) messages.

To enable subscriber tracing, you must configure the following:

- **Set Subscribers**—Set the number of number of subscribers that the security device actively traces concurrently. The default number of simultaneous active traces is three (3).

- **Specify Log Bytes**—Specify the number of bytes of data to log for a GTP-U packet. The default value is zero, meaning that the device does not log any content from a GTP-U packet. When you enter a number other than zero, the security device sends the logged packets to an external server (such as Syslog) dedicated to Lawful Interception operations.

- **Set ID**—For each subscriber you want to trace, enter their ID number and select Based on IMSI or Based on MSISDN.

**EXAMPLE: CREATING A GTP OBJECT**

1. In Object Manager, select GTP Objects, then click the Add icon in the main display area. The New GTP Object dialog box appears.

2. In the Info tab, configure the following settings:

   - For Name, enter GPRS1, then enter a color and comment for the object.

   - Select Sequence Number Validation.
3. In the GTP navigation tree, select Traffic Logging/Counting. Configure the following:
   - For Traffic Counters, select Count by Message.
   - Select Basic for the following message types: Log Forwarded Packets, Log Dropped Packet Due to Type/Length/Version, and Log Dropped Packet Due to Invalid State.
   - Leave all other defaults.

4. In the GTP navigation tree, select IMSI Prefix and APN Filtering. Click the Add icon to display a new IMSI Prefix and APN Filter Entry dialog box. Configure the following, then click OK:
   - For APN, enter mobiphone.com.mnc123.mcc456.gprs.
   - Select MCC-MNC and enter the code 24656.
   - For Selection Mode, select Mobile Station, Network, and Verified.

5. In the GTP navigation tree, select Subscriber Tracing.
   - For Maximum Number of Simultaneous Active Traces, enter 2.
   - For Number of Bytes to Be Saved to Log, enter 1020.

6. Click the Add icon to display a New Subscriber ID dialog box. Configure the following, then click OK:
   - For ID, enter 345678.
   - For ID Type, select Based on IMSI.

7. Click OK to save the new Subscriber ID, then click OK to save the GPRS1 object.

Configuring Service Objects

Service objects represent the IP traffic types for existing protocol standards. Security devices monitor and manage network traffic using these protocols. NetScreen-Security Manager includes predefined service objects for most standard services. You can also create custom service objects to represent services that are not included in the list of predefined service objects, or to represent a custom service running on your network.

You use service objects to create protected resources and specify the type of service within a Security Policy:

- In a protected resource, select a service or group of services to define the types of traffic you are permitting to and from the resource.
In individual rules within a firewall or IDP rulebase, select one or more services or groups of services to define the types of IP traffic to which the rule applies. The action of the rule applies when the security device detects packets that use the specified service type.

**Viewing Predefined Services**

You can view predefined services in a tree or table format. The Service Tree displays services in a tree format, with service groups and individual services. The Service Table displays services in a table format, and includes the following details:

<table>
<thead>
<tr>
<th>Table 26: Service Table Tab Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Type</td>
</tr>
<tr>
<td>Timeout</td>
</tr>
<tr>
<td>Category</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Non-ICMP Src Port</td>
</tr>
<tr>
<td>Non-ICMP Dst Port</td>
</tr>
<tr>
<td>Comment</td>
</tr>
</tbody>
</table>

To view service object properties, double-click a service object. In addition to the service name, category, and service timeout value, you can view the following service settings:

- For Non-ICMP services, the service object displays the protocol ID, source port range, and destination port range.
- For ICMP services, the General tab displays the Internet Control Message Protocol (ICMP) type and code.
For Sun-RPC services, the Sun-RPC tab displays the Sun Microsystems program identifiers. Sun Remote Procedure Call (Sun-RPC), also known as Open Network Computing (ONC) RPC, enables a program running on one host to call procedures in a program running on another host. Because of the large number of RPC services and the need to broadcast, the transport address of an RPC service is dynamically negotiated based on the service’s program number and version number. Several binding protocols are defined for mapping the RPC program number and version number to a transport address.

NOTE: The transport address is comprised of the port number of the server, the program ID, and the version number.

NetScreen-Security Manager and security devices support 13 Sun-RPC predefined services. To permit or deny all Sun-RPC requests, include the Sun-RPC-Any service in a firewall or IDP rule; to permit or deny a Sun-RPC request by specific program number, include that service (or create a custom service) in the rule.

For MS-RPC services, the MS-RPC tab displays the Microsoft universal unique identifiers (UUIDs). Microsoft Remote Procedure Call (MS-RPC) is the Microsoft implementation of the Distributed Computing Environment (DCE) RPC. Like the Sun-RPC, MS-RPC enables a program running on one host to call procedures in a program running on another host. Because of the large number of RPC services and the need to broadcast, the transport address of an RPC service is dynamically negotiated based on the service program’s Universal Unique Identifier (UUID).

NetScreen-Security Manager and security devices support 27 MS-RPC predefined services and 3 MS-RPC predefined service groups. To permit or deny all MS-RPC requests, include the MS-RPC-Any service in a firewall or IDP rule; to permit or deny an MS-RPC request by specific UUID, include that service (or create a custom service) in the rule.

You can view details for a predefined service object, but you cannot edit that service object.

**Creating Custom Services**

You can create custom service objects to represent protocols that are not included in the predefined services or to meet the unique needs of your network.

NOTE: Sun-RPC protocols and regular TCP/UDP/ICMP protocols cannot be in the same service object. MS-RPC protocols and regular TCP/UDP/ICMP protocols cannot be in the same service object.

To add a service object, in the Object Manager, select **Service Objects > Custom Service Objects**. In the main display area, click the Add icon and select Service to display the New Service dialog box. Configure the following parameters:

- **Name**—Enter a name for the service.
- **Timeout**—Select the session timeout after which an inactive session is removed.
Never. The session does not timeout.

Default. Use the default timeout for the selected protocol. The default timeout for TCP connections is 30 minutes. The default timeout for UDP connections is 1 minute.

User-defined. Enter a session timeout value. The maximum timeout value for TCP and UDP connections is 2160 minutes.

Color—Select a color to represent this service object in the NetScreen-Security Manager UI.

Comment—Add a comment, if desired.

Add the service entry:

For ICMP services, in the General tab click the Add icon. Enter the ICMP type and code, then click OK. For information about ICMP type, see the NetScreen-Security Manager Online Help.

For Sun-RPC services, select the Sun-RPC tab, then click the Add icon. Enter high and low program identifiers, then click OK. You can add up to eight program ranges; ensure that the Program High value is greater than or equal to the Program Low value.

NOTE: For the complete list of the Sun Microsystems Program IDs and Microsoft UUIDs, refer to the Juniper Networks ScreenOS online help.

For MS-RPC services, select the MS-RPC tab, then click the Add icon. Enter a UUID, then click OK. A UUID is 36 characters.

For other non-ICMP services, in the NON-ICMP Service Entries area, click the Add icon. Select the protocol type and configure the source and destination ports, the click OK. To create a service object that uses multiple ports for the same service, add two service entries with different ports.

Service Object Groups

You can group services together as a service object group, then use that group in Security Policies and VPNs to simplify administration. Each service object can be referenced by multiple service object groups. Service object groups can contain both predefined and custom service objects, as well as other service object groups.

To add a service object group:

1. In the navigation tree, select Object Manager > Service Objects.

2. In the main display area, click the Add icon and select New > Group. The new Service Group dialog box appears.

3. Enter a name, color, and comment for the service object group.

NOTE: Service object group names cannot be the same as service object names.
4. In the Non-members area, select the service objects or service object groups you want to add to the group (hold CTRL to select multiple objects), then click Add.

5. Click OK.

The new service object group appears in the Service Tree and Service Table tabs.

**EXAMPLE: CREATING A CUSTOM SERVICE AND GROUP**

In this example, you create a custom service object to represent the Ident service and a custom service group that includes this service.

To create the custom Ident service:

1. In the main navigation tree, select **Object Manager > Service Objects > Custom Service Objects**.

2. In the main display area, click the Add icon and select Service. The New Service dialog box appears.

3. Configure the following:
   a. For Name, enter Ident
   b. For Timeout, select Default.
   c. For Color, select blue.
   d. Enter a Comment, if desired.

4. In the Non-ICMP Services Entries area, click the Add icon and select TCP. The New Service Entry dialog box appears. Configure the following:
   a. For Source Port, select Range.
   b. For Source Port Range, enter 0 to 65535.
   c. For Destination Port, select Specific.
   d. For Specific Port, enter 113.

5. Click OK to save the new service entry, then click OK again to save the new service object.

6. In the main display area, click the Add icon and select Group. The New Service Group dialog box appears. Configure the following:
   a. For Name, enter Remote Mail.
   b. For Color, select pink.
   c. Enter a Comment, if desired.
   d. In the non-members area, select the following services (press and hold Ctrl to select multiple services):
Configuring Service Objects

- FTP
- HTTP
- Ident
- MAIL
- POP3
- TELNET

e. Click Add to add the services as members of the group, then click OK to save the new service group.

EXAMPLE: CREATING A CUSTOM SUN-RPC SERVICE
In this example, you create a service object called my-sunrpc-nfs to use the Sun RPC Network File System, which is identified by two Program IDs: 100003 and 100227. Because Sun RPC services use dynamically negotiated ports, you can not use regular service objects based on fixed TCP/UDP ports to permit them in security policy. Instead, you must create sun rpc service objects using program numbers. For example, NFS uses two program numbers: 100003 and 100227. The corresponding TCP/UDP ports are dynamic. To permit the program numbers, you create a sun-rpc-nfs service object that contains these two numbers. The ALG maps the program numbers into dynamically negotiated TCP/UDP ports, and permits or denies the service based on a policy you configure.

To create the Sun-RPC service:

1. In the main navigation tree, select Object Manager > Service Objects > Custom Service Objects.

2. In the main display area, click the Add icon and select Service. The New Service dialog box appears.

3. Configure the following:
   a. For Name, enter my-sunrpc-nfs
   b. For Timeout, select Default.
   c. For Color, select blue.
   d. Enter a Comment, if desired.

4. Select the Sun-RPC tab.
   a. Configure the first service entry. Click the Add icon to display the New Service Entry dialog box, configure the following, then click OK:
      - For Program Low, enter 100003.
      - For Program High, enter 100003.
b. Configure the second service entry. Click the Add icon to display the New Service Entry dialog box, configure the following, then click OK:

- For Program Low, enter 100227.
- For Program High, enter 100227.

5. Click OK again to save the new service object.

EXAMPLE: CREATING A CUSTOM MS-RPC SERVICE

In this example, you create a service object called my-ex-info-store that includes the UUIDs for the MS Exchange Info Store service. Because MS RPC services use dynamically negotiated ports, you cannot use regular service objects based on fixed TCP/UDP ports to permit them in a security policy. Instead, you must create MS RPC service objects using UUIDs. The MS Exchange Info Store service, for example, uses the following four UUIDs:

- 0e4a0156-dd5d-11d2-8c2f-00c04fb6bcde
- 1453c42c-0fa6-11d2-a910-00c04f990f3b
- 10f24e8e-0fa6-11d2-a910-00c04f990f3b
- 1544f5e0-613c-11d1-93df-00c04fd7bd09

The corresponding TCP/UDP ports are dynamic. To permit them, you create an ms-exchange-info-store service object that contains these four UUIDs. The ALG maps the program numbers into dynamically negotiated TCP/UDP ports based on these four UUIDs, and permits or denies the service based on a rule you configure.

To create the MS-RPC service:

1. In the main navigation tree, select Object Manager > Service Objects > Custom Service Objects.
2. In the main display area, click the Add icon and select Service. The New Service dialog box appears.
3. Configure the following:
   a. For Name, enter my-ex-info-store
   b. For Timeout, select Default.
   c. For Color, select blue.
   d. Enter a Comment, if desired.
4. Select the MS-RPC tab. Configure a service entry for each of the following UUIDs:
   - 0e4a0156-dd5d-11d2-8c2f-00c04fb6bcde
   - 1453c42c-0fa6-11d2-a910-00c04f990f3b
5. Click OK to save the new service object.

**Editing and Deleting Service Objects**

You can edit a service object by right-clicking on the object and selecting **Edit**. You can also delete a service object by right-clicking on the object and selecting **Delete**. For more information on editing and deleting service objects, refer to the NetScreen-Security Manager Online Help.

**Replacing Service Objects**

You can replace a service object by right-clicking on the object and selecting **Replace With**. Replacing service objects eases the need to make redundant changes to a service object that is referenced in multiple security policies. When replacing service objects however, you want to keep the following in mind:

- There is no validation check when replacing service objects; an error appears for any service objects that are not valid for specific policies, for example, you cannot assign a SUN-RPC-ANY service object to an IDP policy.

- You cannot replace a service object with a service group object that contains the replaced service object.

- You cannot undo or roll back a replace with operation.

**NOTE:** Replacing service objects only applies to those objects in the domain in which you are working. Custom Services created in Global Domain will not be avaiavle for the Replace With operations in subdomains.

After replacing service objects, it is good practice to check your security policies for any errors that may result. You can always edit or remove any duplicate objects in the security policy.

**EXAMPLE: REPLACING HTTP WITH HTTPS**

In this example, you want to replace all references to HTTP with HTTPS in your security policies.

To replace HTTP with HTTPS:

1. In the navigation tree, open the Object Manager and click on **Service Objects** to open the service object tree.

2. Click on **Predefined Service Objects**.

3. In the Service Tree or Service Table, right-click on the HTTP service object and select **Replace With**. The Replace With wizard appears displaying a list of objects you can replace the selected service object with.
4. Select the HTTPS service object. Click **Next**. The wizard next displays the objects affected by the Replace With operation.

As an optional step, you can delete any replaced custom service objects by clicking on them and then selecting **Delete Replaced Object**.

**NOTE:** You cannot delete a predefined service object.

5. Click **Finish**.

**Configuring Authentication Servers**

An authentication server provides authentication services for NetScreen-Security Manager administrators and remote access services (RAS) users on your network. The information stored in an authentication server determines the privileges of each administrator.

When the security device receives a connection request that requires authentication verification, the device requests an authentication check from the external auth server specified in the policy, L2TP tunnel configuration, or IKE gateway configuration. The device then acts as a relay between the user requesting authentication and the authentication server granting authentication.

In NetScreen-Security Manager, an auth server is an object used in Security Policies, IKE gateways, and L2TP tunnels. Each security device includes a default authentication server; however, to enable an external RADIUS, SecureID, or LDAP server to provide authentication, you must configure an external authentication server object. You can also configure a RADIUS authentication server object to provide authentication for the global domain and each subdomain. For information about configuring a RADIUS server, see “Configuring a RADIUS Authentication Server” on page 292.

**NOTE:** You must also define routes that direct authentication requests to the RADIUS, SecureID, and LDAP servers.

To configure general authentication server object properties, in the main navigation tree, select **Object Manager > Authentication Servers** then click the Add icon. The General, Redundancy, and Identity tabs are the same for all server types; in the Server Type tab, select the authentication server type (RADIUS, SecureID, LDAP) to configure specific settings for that server type.

**Configuring General Authentication Server Settings**

In the General tab, configure a name, color, and comment that uniquely identify the object, then specify the IP address of the main authentication server; this is the IP address of the server that handles authentication requests.

You can also configure an authentication timeout (default is 10 minutes) to control the number of minutes before an authentication check times out. Timeouts affect the following user types differently:
Auth user. The timeout countdown begins after the first authenticated session
completes. If users initiate a new session before the countdown reaches the
timeout threshold, they do not need to reauthenticate and the timeout
countdown resets. The default timeout value is 10 minutes, and the maximum
is 255 minutes. You can also set the timeout value at 0 so that the
authentication period never times out.

Admin user. If the length of idle time reaches the timeout threshold, the
security device terminates the admin session. To continue managing the
device, the admin must reconnect to the device and re authenticate. The default
timeout value is 10 minutes, and the maximum is 1000 minutes. You can also
set the timeout value at 0 so that an admin session never times out.

NOTE: User authentication timeout is not the same as session idle timeout. If no
activity occurs in a session for a predefined length of time, the security device
automatically removes the session from its session table.

Configuring Authentication Server Redundancy

In the Redundancy tab, you can configure backup server to handle authentication
requests if the primary server fails. For RADIUS servers only, you can also configure
a secondary backup server (this option is not supported for SecureID servers).

For RADIUS and LDAP servers only, you can configure a Failover Revert Interval that
determines how long the device uses a backup server before attempting to use the
primary server again. To configure the interval, enter the number of seconds (1 to
86400); to disable the failover revert, set the interval to 0 (the device continues to
use the backup server indefinitely). The interval countdown begins when the device
fails over from the primary auth server to the backup or secondary backup server
(RADIUS only).

Configuring Authentication for User Types

In the Identity tab, configure the user types that the authentication server supports:

- Admin Users
- Firewall Auth Users
- XAuth Users
- 802.1x Users
- L2TP Users

For RADIUS servers, you can also configure the optional domain name checking
and domain name stripping settings, as detailed in the following sections.

Domain Name Checking

Use domain name checking to authenticate users from a specific domain. This
setting is optional and is not required to configure a RADIUS authentication server.
To configure, for Domain to Check In Username, enter the domain name (up to 45 characters). For each user authenticating to the server, the server compares the domain name in the username to specified domain (the domain is read as a string from right to left to the first @ character).

To authenticate usernames from all domains, leave this option unconfigured (blank).

Domain Name Stripping
Use domain name stripping to remove the domain name from usernames before sending to the authentication server. This setting is optional and is not required to configure a RADIUS authentication server. However, you might need to configure this setting when implementing a new RADIUS server with an existing network and established usernames.

To configure:

- For Separator Character, enter the separator character used in the usernames.
- For Separator Character Occurrence, enter the number of times (0 to 10) the separator character occurs in the username.

When a user attempts to authenticate, the device examines the username from right to left, then strips domain name information for the specified number of separator characters before sending the username onto the authentication server.

For example, when the Separator Character is @ and the Separator Character Occurrence is 2, the device handles the username `user1@mygrp.abc@myco.com` by stripping the characters `@mygrp.abc@myco.com` and sending only the characters `user1` to the authentication server.

If the device does not locate the separator character in the username, it does not strip the domain name from the username (usernames are passed to the authentication server as-is). Conversely, if the number of specified separator characters exceeds the number of separators found in a username, the device strips domain name information to the number of separators found (when reading right to left).

Configuring Authentication Server Types
In the Server Type tab, select the authentication server type (RADIUS, SecureID, LDAP) to configure specific settings for that server type:

- For RADIUS, see “Configuring a RADIUS Authentication Server” on page 292.
- For SecureID, see “Configuring a SecurID Authentication Server” on page 296
- For LDAP, see “Configuring a RADIUS Authentication Server” on page 292
Configuring a RADIUS Authentication Server

The Remote Authentication Dial-In User Service (RADIUS) is a protocol for an authentication server that can support up to tens of thousands of users. The security device acts as a RADIUS client that authenticates users. When users log in, the RADIUS client (the security device) prompts them for their user name and password, then compares these values with the values stored in the RADIUS database. If the values match, the RADIUS client authenticates the user and permits access to the appropriate network services.

For a RADIUS authentication server object, configure the following:

- **RADIUS Port**—The port number on the RADIUS server to which a security device sends authentication requests. The default port number is 1645.

- **RADIUS Secret**—The secret (password) shared between a security device and the RADIUS server. The RADIUS server uses the shared secret to generate a key to encrypt traffic between the security device and the RADIUS server. The security device uses the shared secret to encrypt the user’s password that it sends to the RADIUS server.

- **RADIUS Retry Timeout**—The interval (in seconds) that a security device waits before sending another authentication request to the RADIUS server if the previous request does not elicit a response. The default is three seconds.

- **RADIUS Retries**—The number of unanswered requests (access and accounting) that a security device sends before it considers the RADIUS server unreachable and fails over to a backup server. To configure, enter the number of retries (1 to 20); the default is three.

- **RADIUS Compatible with RFC 2138**—When selected, enables the authentication server to comply with RFC 2138, an older RADIUS standard, with the following considerations:
  - For operations where RFC 2865/66 and RFC 2138 are mutually exclusive, the server complies with RFC 2138 only.
  - For operations where RFC 2865/66 and RFC 2138 are both supported, the server complies with all three RFCs.
When unselected (default), the server is compatible only with the current RADIUS standards RFC 2865 and 2866.

- Enable Sending Calling-Station-ID—When selected, the security device transmits the calling station ID within the access or accounting request to the RADIUS authentication server. Because the ID identifies the originator of the call (either the IKE IP address for XAuth or the phone number of the user originating the call), you might not want to send this information to the server. By default, this option is disabled; the device does not send the calling station ID to the server.

- Length of Account Session ID Attribute—The byte length of the account-session-id, which uniquely identifies the accounting session. By default, the byte length is 11, and follows the format NS-xxxxxxxx. Because some RADIUS servers do not properly accept an 11-byte account session ID, you might want to configure a lower byte length that does not include the “NS-“ prefix. To configure, enter a byte length from 6 to 10.

**Supported User Types**

A RADIUS server supports the following user types:

- Auth users
- L2TP users (authentication and remote settings)
- XAuth users (authentication and remote settings)
- Admin users (authentication and privilege assignments)
- User groups

A RADIUS server **does not** support IKE users.

**RADIUS Access-Challenge**

When a user attempts to log in using telnet, a security device can process access-challenge packets from an external RADIUS server. Access-challenge is an additional authentication level. After a username and password has been authenticated, the RADIUS server sends an access-challenge to the security device, which forwards the challenge to the user. When the user replies, the device sends a new access-request with the user’s response to the RADIUS server; if the user’s response is correct, the authentication process concludes successfully.

---

**NOTE:** Juniper Networks does not support access-challenge with L2TP.

---

**Juniper Networks Dictionary File**

A dictionary file defines vendor-specific attributes (VSAs) that you load onto a RADIUS server. After you define the VSA values, the security device can query those values when a user logs on to the device.
You must load a Juniper Networks dictionary file to enable the RADIUS server to support NetScreen-specific attributes as admin privileges, user groups, and remote L2TP and XAuth IP address, and DNS and WINS server address assignments. You do not need to load Juniper Networks dictionary file to enable RADIUS to make IP address assignments (Juniper Networks uses the standard RADIUS attribute for IP address assignments).

Juniper Networks provides two dictionary files: one for Cisco RADIUS servers and one for Funk Software RADIUS servers:

- For Funk Software RADIUS server dictionary file, go to http://www.juniper.net/customers/csc/research/netscreen_kb/downloads/dictionary/funk_radius.zip
- For Cisco RADIUS server dictionary file, go to http://www.juniper.net/customers/csc/research/netscreen_kb/downloads/dictionary/cisco_radius.zip

If using a Microsoft RADIUS server, there is no dictionary file. You must configure it as outlined in Using a Windows NT Domain / Active Directory for User Authentication Security Devices, which you can download from the Juniper customer support site.

Each Juniper Networks dictionary file contains the following specific information:

- Vendor ID—The Juniper Networks vendor ID (VID; also called an “IETF number”) is 3224. The VID identifies a specific vendor for a particular attribute. Some types of RADIUS server require you to enter the VID for each attribute entry, while other types only require you to enter it once and then apply it globally. Refer to your RADIUS server documentation for further information.

- Attribute Name—The attribute names describe individual NetScreen-specific attributes, such as NS-Admin-Privilege, NS-User-Group, and NS-Primary-DNS-Server.

- Attribute Number—The attribute number identifies an individual vendor-specific attribute.

- Attribute Type—The attribute type identifies the form in which attribute data (or “value”) appears—a string, an IP address, or an integer.

The RADIUS server automatically receives the above information when you load the Juniper Networks dictionary file onto it. To make new data entries, you must manually enter a value in the form indicated by the attribute type.

EXAMPLE: CONFIGURING A RADIUS AUTH SERVER

In the following example, you define an auth server object for a RADIUS server. You specify its user account types as auth, L2TP, and XAuth. You name the RADIUS server “radius1” and accept the ID number that the security device automatically assigns it. You enter its IP address, which is 10.20.1.100; and change its port number from the default port number (1645) to 4500. You define its shared secret as “A56htYY97kl”. You change the authentication timeout value from the default (10 minutes) to 30 minutes and the RADIUS retry timeout from 3 seconds to 4 seconds. You also assign its two backup servers the IP addresses 10.20.1.110 and 10.20.1.120.
In addition, you load the Juniper Networks dictionary file on the RADIUS server so that it can support queries for the following vendor-specific attributes (VSAs): user groups, admin privileges, remote L2TP and XAuth settings.

Figure 62: Configure RADIUS Auth Server

The security device sends auth, L2TP, and XAuth authentication requests to the primary RADIUS server, “radius1”, at 10.20.1.100.

If the security device loses network connectivity with the primary RADIUS server, the device redirects authentication requests to backup1 at 10.20.1.110.

If the security device cannot reach backup1, it redirects authentication requests to backup2 at 10.20.1.120.

1. In the main navigation tree, select **Object Manager > Authentication Servers** and click the Add icon. Enter a name, color, and comment for the authentication server.

2. Configure the RADIUS servers:
   - For Main Server, enter the IP **10.20.1.100**
   - For Primary Backup Server, enter IP **10.20.1.110**
   - For Secondary Backup Server, enter IP **10.20.1.120**

3. For timeout, enter **30**.

4. Select the following:
   - For Firewall Auth Users
   - For XAuth Users
   - For L2TP Users

5. For Server Type, select **RADIUS**.

6. Configure the RADIUS server properties:
   - For server port, enter **4500** (default is 1645)
   - For secret, enter **A56hYY97kl**
   - For retry timeout, select **4**.
7. Click **OK** to save the RADIUS authentication server object.

8. Load the Juniper Networks dictionary file on the RADIUS server.

### Configuring a SecurID Authentication Server

Security devices also support the RSA SecurID system. The device acts as a SecurID client, forwarding authentication requests to the external server for approval and relaying login information between the user and the server. Each SecurID user has three authentication credentials:

- **User Name**
- **Personal identification number (PIN)**
- **Authenticator**—a SecurID issued device with an LCD screen that displays a token code, a randomly generated string of numbers that changes every minute. The authenticator uses an algorithm known only by RSA to create the token code that appears in LCD screen; when users enter their username, their PIN, and the token code from their authenticator, the RSA ACE server also performs the same algorithm, generating a match between the server and the user.

When users log in, the SecurID client (the security device) prompts them for their user name, their PIN, and the current token code. The device compares the user input against value generated by the RSA ACE server algorithm. If the values match, the authentication is successful.

For a SecurID authentication server object, you must configure the following:

- **Authentication Port**—The port number on the SecurID ACE server to which the security device sends authentication requests. The default port number is 5500.
- **Encryption Type**—The algorithm used for encrypting communication between the security device and the SecurID ACE server (SDI or DES).
- **Client Retries**—The number of times that the SecurID client (the security device) tries to establish communication with the SecurID ACE server before aborting the attempt.
- **Client Timeout**—The length of time in seconds that the security device waits between authentication retry attempts.
- **Use Duress**—An option that prevents or allows use of a different PIN number. When this option is enabled, and a user enters a previously determined duress PIN number, the security device sends a signal to the SecurID ACE server, indicating that the user is performing the login against his or her will, possible under duress. The SecurID ACE server permits access that one time, then denies any further login attempts by that user until he or she contacts the SecurID administrator. Duress mode is available only if the SecurID ACE server supports this option.
Supported Users
A SecurID Ace server supports the following types of users and authentication features:

- Auth users
- L2TP users (user authentication; L2TP user receives default L2TP settings from the security device)
- XAuth users (user authentication; no support for remote setting assignments)
- Admin users (user authentication; admin user receives default privilege assignment of read-only)

A SecurID ACE server can store L2TP, XAuth, and device admin user accounts for authentication purposes; but it cannot assign L2TP, XAuth remote settings, or device admin privileges.

Configuring an LDAP Authentication Server
Lightweight Directory Access Protocol (LDAP) a protocol for organizing and accessing information in a hierarchical structure resembling a branching tree. LDAP is used to locate resources, such as organizations, individuals, and files on a network, and helps authenticate users attempting to connect to networks controlled by directory servers.

To create an LDAP authentication server object, configure the following:

- LDAP Server Port: The port number on the LDAP server to which the security device sends authentication requests. The default port number is 389.
- Common Name Identifier: The identifier used by the LDAP server to identify the individual entered in a LDAP server. For example, an entry of "uid" means "user ID" and "cn" for "common name".
- Distinguished Name (dn): The path used by the LDAP server before using the common name identifier to search for a specific entry. (For example, c=us,o=juniper, where "c" stands for "country", and "o" for "organization".)

Supported Users
An LDAP server supports the following types of users and authentication features:

- Auth users
- L2TP users (user authentication; L2TP user receives default L2TP settings from the security device)
- XAuth users (user authentication; no support for remote setting assignments)
- Admin users (user authentication; admin user receives default privilege assignment of read-only)

LDAP servers cannot assign L2TP or XAuth remote settings.
Configuring User Objects

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

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

- **External Users and External User Groups**—Users with accounts that are managed by external devices, such as RADIUS servers. You can use external users and groups to create group expressions (for details, see “Configuring Group Expressions” on page 304).

### Configuring Local Users

Local User Objects represent the user account on your security devices. To add a local user object:

1. In the navigation tree, double-click the Object Manager, select User Objects, then select Local Users. In the main display area, click the Add icon and select **New > User** to display the New Local User dialog box.

2. Enter a name, color, and comment for the local group.

3. Select **Enable** to enable authentication for this user, then configure the authentication methods for the user.
   - **XAuth.** Enables XAuth authentication for this user. If you select this option, you must also enter an XAuth password for the user.
   - **IKE.** Enables IKE authentication using one of the IKE proposals defined in the IKE Proposal Objects. If you select this option, you must also configure the IKE Share limit and authentication token.
   - **Auth.** Enables local authentication against a username and password stored in a security device’s local database. If you select this option, you must also enter an Auth password for the user.
   - **L2TP.** Enables authentication in the L2TP tunnel that the user uses to connect to the device. If you select this option, you must also enter an L2TP password for the user.

4. Click **OK** to save the user object.

### Configuring Local User Groups

Organize local users in groups to add multiple users at one time to a Security Policy, and to manage the members without changing the policy. To add a local user group object:

---

**NOTE:** All passwords handled by NetScreen-Security Manager are case-sensitive.
1. In the navigation tree, double-click the Object Manager, select User Objects, then select Local Users. In the main display area, click the Add icon and select New > Group to display the New Local User Group dialog box.

2. Enter a name, color, and comment for the local user group.

3. Configure the members of the group:
   - To add members, select users from the Non-members list and click Add. Use Ctrl-click to select multiple users, or click Add All to add all users in Non-members list to the group.
   - To remove members, select users in the Members list and click Remove. Use Ctrl-click to select multiple users, or click Remove All to remove all users in Members list from the group.

4. Click OK to save the local user group.

Configuring External Users

External User Objects represent users whose accounts are maintained and authenticated on devices that are not managed by NetScreen-Security Manager, such as an external RADIUS or SecureID server. When an external user is included in a Security Policy (under Authentication rule options), the security device uses the external server to authenticate that user.

To configure an external user:

1. In the navigation tree, double-click the Object Manager, select User Objects, then select External Users. In the main display area, click the Add icon and select New to display the New External User dialog box.

2. Enter a name, color, and comment for the external user.

3. Click OK to save the external user object.

Configuring External User Groups

External User Group objects represent user groups that are managed on non-security devices, such as an external RADIUS or SecureID server. When an external user group is included in a Security Policy (under Authentication rule options), the security device uses the external server to authenticate those users.

To use an external user group in a VPN, however, you must also create local user objects with IKE authentication for each external user. In phase 1 of IKE negotiations, the security device authenticates the external user group using the RADIUS server. In phase 2 of IKE negotiations, the device uses the local user object or local user group for authentication. Typically, you configure the local user object with IKE authentication and a U-FQDN (email address); during phase 2, the device prompts the user for their U-FQDN for authentication.

To add an external user group object:
1. In the navigation tree, select **Object Manager > User Objects > External User Groups**. In the main display area, click the Add icon and select **New** to display the New External Group dialog box.

2. Enter a name for the external user group. The name must match the name of the user group as configured on the external server.

3. Enter a color and comment for the external user group.

4. Configure the authentication methods for the user group:
   - XAuth. Enables XAuth authentication for the user group.
   - Auth. Enables local authentication against a username and password stored in a security device's local database.

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

   - L2TP. Enables authentication in the L2TP tunnel that users in the group use to connect to the device.

5. Click **OK** to save the new group.

**EXAMPLE: USING RADIUS WITH USER GROUPS**
In this example, you configure an external RADIUS auth server named radius1 and define an external auth user group named auth_grp2. You define the external auth user group auth_grp2 in two places: External RADIUS auth server “radius1”, and in NetScreen-Security Manager. For the RADIUS server, you enter the IP address 10.20.1.100 and change its port number from the default port number (1645) to 4500.

Next, you populate the auth user group “auth_grp2” with auth users on the RADIUS server only, leaving the group unpopulated in NetScreen-Security Manager. The members in this group are accountants who require exclusive access to a server at IP address 10.1.1.80. You create an address book entry for the server and name the address “midas.” Finally, you configure a Security Policy that permits only authenticated traffic from auth_grp2 to midas, both of which are in the Trust zone.

1. On the RADIUS server, load the Juniper Networks dictionary file and define auth user accounts. Use the Juniper Networks user group VSA to create the user group auth_grp2 and apply it to the auth user accounts that you want to add to that group.

   **NOTE:** For instructions on loading the dictionary file onto a RADIUS server, refer to the RADIUS server documentation. If you are using a Microsoft IAS RADIUS server, there is no dictionary file to load; you must manually define the correct vendor-specific attributes (VSAs) on the server.

2. In NetScreen-Security Manager, in the main navigation tree, select **Object Manager > Authentication Servers** and click the Add icon. Configure the server:
   - For name, enter **radius1**. Select a color and add a comment, if desired.
b. For Main Server, enter the IP 10.20.1.100; for Primary Backup Server, enter IP 10.20.1.110; for Secondary Backup Server, enter IP 10.20.1.120.

c. For timeout, enter 30.

d. Select **For Firewall Auth Users**.

e. For Server Type, select **RADIUS**, then configure the RADIUS server:
   - For server port, enter 4500 (default is 1645)
   - For secret, enter A56hYY97kl
   - For retry timeout, select 4.

f. Click **OK** to save the RADIUS authentication server object.

3. Configure the External User Group in NetScreen-Security Manager:

   a. In the Object Manager, select **User Objects > External User Groups**.

   b. Click the Add icon to display the New External User Group dialog box. Configure the following, then click **OK**:
      - For Name, enter auth_grp2.
      - For Color, select **red**.
      - For Comment, enter **Accountant Access**.
      - Enable **Auth**.

4. Add the Address Object that represents the Accounting Server:

   a. In the Object Manager, select **Address Objects**. Click the Add icon and select **Host**. The New Host dialog box appears.

   b. Configure the following, then click **OK**:
      - For Name, enter Midas.
      - For Color, select orange.
      - For Comment, enter **Accounting Server**.
      - Select **IP**, then enter the IP Address 10.1.1.80.

5. Configure a firewall rule to use the RADIUS authentication server object to authenticate traffic between the external user group and the Midas server, as shown in Figure 63.
Configuring VLAN Objects

Use VLAN objects to limit rule matching to packets within a particular VLAN.

VLAN objects can either target a specific VLAN tag, or a range of VLAN tags. You can use more than one VLAN object in a rule.

VLAN objects have the following components:

- **Name**: What the object is called in the NSM UI.
- Comment and Color: Useful for organizing and explaining the object to other users. Have no effect on the object in the system.
- ID Type: Specify whether the object will cover a single VLAN tag or a range of VLAN tags.
- Specific and Low/High: For a single VLAN tag, specify the tag. For a range of VLAN tags, specify the lowest and highest values in the range.

See Setting VLAN Tags for IDP Rules on page 361 for information on using VLAN tags in rulebases.

Configuring IP Pools

An IP pool object contains IP ranges (a range of IP addresses within the same subnet). You use IP Pool objects to assign IP addresses to L2TP users in L2TP VPNs or local users on a specific device. The IP pool you select for the VPN or the local user determines the range of IP addresses the device can assign to the L2TP RAS user when the user connects to the L2TP VPN.

**NOTE:** For more information about configuring XAuth and L2TP local users on a device, see “NetScreen-Security Manager: Configuring Firewall/VPN Devices“.

An IP range includes the following:

- Start IP—The beginning of the range of IP addresses included in the pool, inclusive. The Start IP must always be lower than the End IP.
- End IP—The end of the range of IP addresses included in the pool, inclusive. The End IP must always be higher than the Start IP.

Using Multiple IP Ranges

An IP Pool object can contain multiple, non-sequential IP ranges. You might need to use multiple ranges to accommodate large numbers of RAS users in a VPN.

You can configure up to 256 IP ranges within a single IP Pool object. You can add any number of IP Pool objects.

**NOTE:** Devices running ScreenOS 5.1 or earlier versions do not support multiple IP pool ranges. When you include a multi-range IP pool object in a device configuration or VPN for a device running ScreenOS 5.1 or earlier version, the device automatically uses the first IP range defined in the IP Pool object.

To modify or delete an IP range from an IP Pool object, you must first ensure that no IP within the range is currently in use by any managed device. If you change or delete an IP range that contains a used IP address, the device using the IP generates an error during device update (error message appears with the Job Manager dialog box for the update).
EXAMPLE:  CONFIGURING AN IP POOL OBJECT
In this example, you configure an IP pool with the ranges 1.1.1.1-1.1.1.10 and 2.2.2.2-2.2.2.20.

1. In the navigation tree, select **Object Manager > IP Pools**.
2. In the main display area, click the Add icon. The New IP Pool dialog box appears. Configure as follows:
   - For Name, enter **L2TP User Group 1**.
   - For Color, select **orange**.
   - For Comment, enter IPs for usergrp 1.
3. In the IP Pool dialog box, click the Add icon to configure the first IP pool range. The New IP Pool Name dialog box appears. Configure the Start IP and End IP, then click **OK**:
   - For Start IP, enter **1.1.1.1**.
   - For End IP, enter **1.1.1.10**.
4. In the IP Pool dialog box, click the Add icon to configure the second IP pool range. The New IP Pool Name dialog box appears. Configure the Start IP and End IP, then click **OK**:
   - For Start IP, enter **2.2.2.2**.
   - For End IP, enter **2.2.2.20**.
5. Click **OK** again to save the IP Pool object and return to Object Manager.

Configuring Group Expressions

Group expressions are statements that set conditions for authentication requirements, enabling you to combine multiple external user objects. You can create group expressions using the operator OR, AND, or NOT to combine user objects, user group objects, or other group expressions to define:

- Alternatives for authentication (“a” OR “b”)
- Requirements for authentication “a” AND “b”)
- Exclusions of a user, user group, or another group expression (NOT “c”).

**NOTE:** The user and user groups you reference in the group expressions must be external users that are stored on an external RADIUS server. (A RADIUS server enables a user to belong to more than one user group).

The operators have different meanings depending on the type of user object you are using in the Security Policy, as listed in Table 27.
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:

### User Objects

<table>
<thead>
<tr>
<th>Operator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>OR</strong></td>
<td>If the Security Policy defines authentication for “a” or “b” user objects, the security device authenticates the user if it is either “a” or “b”.</td>
</tr>
<tr>
<td><strong>AND</strong></td>
<td>Requires one of the two objects in the expression to be either a user group or a group expression (a single user cannot be both user “a” and user “b”). If the Security Policy defines authentication for “a” AND a member of group “b”, the security device authenticates the user only if those two conditions are met.</td>
</tr>
<tr>
<td><strong>NOT</strong></td>
<td>If the Security Policy defines authentication for any user object that is not the “c” user (NOT “c”), the security device authenticates all users except the “c” user.</td>
</tr>
</tbody>
</table>

### User groups

<table>
<thead>
<tr>
<th>Operator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>OR</strong></td>
<td>If the Security Policy defines authentication for user group “a” or user group “b”, the security device authenticates the user if it belongs to either “a” or “b” user group.</td>
</tr>
<tr>
<td><strong>AND</strong></td>
<td>If the Security Policy defines authentication for user group “a” AND user group “b”, the security device authenticates the user only if it belongs to both user groups.</td>
</tr>
<tr>
<td><strong>NOT</strong></td>
<td>If the Security Policy defines authentication for any user group that is not group “c” (NOT “c”), the security device authenticates all users except those that belong to the “c” user group.</td>
</tr>
</tbody>
</table>

### Group expressions

<table>
<thead>
<tr>
<th>Operator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>OR</strong></td>
<td>If the Security Policy defines authentication for user objects that match the description of group expression “a” OR group expression “b”, the security device authenticates the user if either group expression references that user.</td>
</tr>
<tr>
<td><strong>AND</strong></td>
<td>If the Security Policy defines authentication for user objects that match the description of group expression “a” AND group expression “b”, the security device authenticates the user only if both group expressions reference that user.</td>
</tr>
<tr>
<td><strong>NOT</strong></td>
<td>If the Security Policy defines authentication for user objects that do not match the description of group expression “c” (NOT “c”), the security device authenticates all users except those that match the group expression.</td>
</tr>
</tbody>
</table>
For NOT expressions, use Operand 1 to select the user object, group, or expression that cannot be present for a successful match. Because the operation is exclusion, you do not need to configure Operand 2.

For AND expressions, use Operand 1 and Operand 2 to select the two user object, group, or expression that must be present for a successful match.

For OR expressions, use Operand 1 and Operand 2 to select the two user object, group, or expression, one of which must be present for a successful match.

5. Click OK. The group expression object appears in the Object Manager.

After you have created a group expression object, you can use that object in the Authentication rule options. For details, see “Configuring Firewall Rule Options” on page 335.

EXAMPLE: CREATING A GROUP EXPRESSION

In this example, you configure a group expression to authenticate all users that belong to your Sales group and your Marketing group, then add the expression to a Security Policy that provides access to your protected networks.

1. First, create two external user group objects: one to represent the Sales users and the other to represent the Marketing users, as shown in Figure 65.

Figure 65: Configure External User Groups for Sales and Marketing

<table>
<thead>
<tr>
<th>External User Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Marketing Group</td>
</tr>
<tr>
<td>Sales Group</td>
</tr>
</tbody>
</table>

2. Next, create a group expression object that reference both the Sales and Marketing group, as shown in Figure 66.
3. Finally, add the group expression object to your firewall rule in the Authentication rule option, as shown in Figure 67.

Configuring Remote Settings

A remote settings object defines the DNS and WINS servers that are assigned to L2TP RAS users after they have connected to the L2TP tunnel. You can use remote settings objects in an L2TP VPN, and when configuring a local user on a specific device.

NOTE: For information about configuring XAuth and L2TP local users on a device, see “NetScreen-Security Manager: Configuring Firewall/VPN Devices”.
Security devices incorporate DNS (domain name server) and WINS support to permit the use of domain names as well as IP addresses for identifying locations. A DNS or WINS server keeps a table of the IP addresses associated with domain names. Using DNS or WINS, you can reference locations by their domain name (www.juniper.net) in addition to using a routeable IP address (such as 209.125.148.136).

Before you can use DNS or WINS for domain name/address resolution in a VPN, you must create remote settings for the DNS or WINS servers (primary and secondary).

To configure a remote setting, select Remote Settings and click the Add icon. Enter a name, color, and comment for the object, then configure the following parameters:

- **DNS1**—Enter the IP address of the primary DNS server.
- **DNS2**—Enter the IP address of the secondary DNS server.
- **WINS1**—Enter the IP address of the primary WINS server.
- **WINS2**—Enter the IP address of the secondary WINS server.

### Configuring NAT Objects

A global NAT object contains references to device-specific NAT configurations, enabling multiple devices to share a single object.

Use the Device Manager to configure NAT for each device, then create a global NAT object that includes the device-specific NAT configuration. The single global NAT object represents multiple device-specific NAT objects; for example, a global DIP represents multiple device-specific DIPs. However, a global NAT object can contain only one device-specific NAT object from the same device.

Use global NAT objects in VPNs; when you install the VPN on a device, that device automatically replaces the global NAT object with its device-specific NAT configuration. Before you configure a shared NAT object, ensure that you have configured the MIP, VIP, or DIP on the device itself.

### Configuring DIP Objects

In Object Manager, select NAT Objects > DIP and click the Add icon. Enter a name, color, and comment for the object, then click the Add icon to specify the device-specific DIP:

- **Device**—Select the security device that includes the DIP.
- **Interface or DIP Group**—Select the interface or DIP group for the device.
  - For interface, select the interface on the device and the dynamic IP address configuration for that interface.
  - For DIP group, select the dynamic IP group configuration for that device.
If no values appear in the pull-down menu for interface, DIP, or DIP group, ensure that you have configured DIP correctly in the Device Manager.

You can add multiple device DIPs to a single global DIP object (one DIP per each device).

Configuring MIP Objects
In Object Manager, select NAT Objects > MIP and click the Add icon. Enter a name, color, and comment for the object, then click the Add icon to specify the device-specific MIP:

- Device—Select the security device that includes the MIP.
- Interface—Select the interface on the device that uses the mapped IP address.
- MIP—Select the mapped IP address configuration for that interface.

If no values appear in the pull-down menu for interface or MIP, ensure that you have configured MIP correctly in the Device Manager. You can add multiple device MIPs to a single global MIP object.

For information about configuring a MIP object and an example, see “NetScreen-Security Manager: Configuring Firewall/VPN Devices”.

Configuring VIP Objects
In Object Manager, select NAT Objects > VIP and click the Add icon. Enter a name, color, and comment for the object, then click the Add icon to specify the device-specific VIP configuration:

- Device—Select the security device that includes the VIP.
- Interface—Select the interface on the device that uses the virtual IP address.
- VIP—Select the virtual IP address configuration for that interface.

If no values appear in the pull-down menu for interface or VIP, ensure that you have configured VIP correctly in the Device Manager. You can add multiple device VIPs to a single global VIP object.

For information about configuring a VIP object and an example, see “NetScreen-Security Manager: Configuring Firewall/VPN Devices”.

Configuring Certificate Authorities
A digital certificate is an electronic means for verifying your identity through the word of a trusted third party, known as a Certificate Authority (CA). NetScreen-Security Manager simplifies creating and managing certificates:

- Use the same CA server for multiple devices. Create a single CA object for each CA server you use, then use that object for those devices.
- Generate a local and CA certificate in one click using SCEP.
Use OCSP to automatically check for revoked certificates (ScreenOS 5.x devices only)

Use a certificate chain that includes a root CA and subordinate CA (CA group)

A CA object represents the CA server you want to use to authenticate the identity of your VPN member. You can use an independent or internal CA server:

- Independent CA server—Owned and operated by an independent CA. The independent CA provides the IP addresses of their CA and CRL servers. You submit a local certificate request to the independent CA and provide your local certificate information.

- Internal CA server—Owned and operated by your company. You provide the IP addresses of the CA and CRL servers and local certificate information.

You can obtain a CA certificate file (.cer) from the CA that issued the local certification, then use this file to create a Certificate Authority object. Then, install this CA certificate on the managed device using NetScreen-Security Manager. Because the CA certificate is an object, however, you can use the same CA for multiple devices, as long as those devices use local certificates that were issued by that CA.

Alternatively, you can use SCEP to configure the device to automatically obtain a CA certificate at the same time it receives the local certificate. For details, see “NetScreen-Security Manager: Configuring Firewall/VPN 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. NetScreen-Security Manager uses the information in the .cer file to automatically complete the Subject Name, Issued By, and Expired On fields.

Complete the remaining settings:

- X.509 Certificate Path Validation Level—X509 contains a specification for a certificate which binds an entity’s distinguished name to its public key through the use of a digital signature.
  - Full. Use full validation to validate the certificate path back to the root.
  - Partial. Use partial validation to validate the certificate path only part of the way to the root.

- Revocation Check
  - Check for revocation. Select this option to enable revocation checking.
Do not check for revocation. Select this option to disable revocation checking.

Revocation Checking Method—If you enabled revocation checking, you can select the checking method to use. If you did not enable revocation checking, these fields are unavailable.

- **CRL.** Use a Certificate Revocation List when you want to keep a local copy of the revoked certificates on the managed device. This method enables the device to check for revoked certificates quickly; to accept the certificate if no revocation information is found, also enable Best Effort.

- **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 security device contacts to request a CA certificate.

- **CA IDENT.** Enter the name of the certificate authority to confirm certificate ownership.
Configuring CRL Objects

A Certificate Revocation List (CRL) identifies invalid certificates. You can obtain a CRL file (.crl) from the CA that issued the local certification and CA certificate for the device, then use this file to create a Certificate Revocation List object.

You must install the CRL on the managed device using NetScreen-Security Manager. Because the CRL is an object, however, you can use the same CRL for multiple devices, as long as those devices use local and CA certificates that were issued by that CA.

Using CRLs

You can use a CRL object in a VPN to check for VPN members using revoked certificates.

Configuring CRLs

After you have obtained a CRL file (.crl) from your CA, use this file to create a Certificate Revocation Object.

In Object Manager, select CRLs, then click the Add icon to display the New CRL dialog box. Enter a name for the CRL, then click Load CRL and load the appropriate .crl file. NetScreen-Security Manager uses the information in the .crl file to automatically complete the Issued By and Expire On fields. Click OK to complete the CRL object.

Configuring Extranet Policies

Extranet policies enable you to configure and manage an extranet device(s) (i.e., third-party router).

EXAMPLE: CONFIGURING AN EXTRANET POLICY OBJECT

In this example, you want to update an existing policy on a third-party router to deny certain ftp traffic from a specific IP address. You can do this by creating a script that performs the required actions when you update the extranet device. You also need to create your rule in an Extranet Policy object.

To create an Extranet Policy object:
1. In the **Object Manager**, select **Extranet Policies**. The New ExtranetPolicyObject window appears.

2. Enter the name of the Extranet Policy, for example, Extranet Policy1. Add a comment in the Comments field.

3. Configure the Extranet Policy object:
   - Click New. The New - Rule window appears.
   - Use the up/down arrow to specify an ID for the rule.
   - Add a comment for the rule.
   - Click **Deny** in the Action field.
   - Select a Source Address in the Source tab.
   - Select a Destination Address in the Destination tab.
   - Select FTP in the Service tab.
   - Select the integer IDs that you created in the Custom Policy Field object in the Options tab.

4. Click OK.

When you create the extranet device in NSM, bind the policy to the appropriate interface and specify the script you want to perform the required update actions. When you update the device, NSM invokes the script. Any XML output appears in the Job Information window.

### Configuring Protected Resources

A protected resource combines network components, network services, a traffic direction, and the security devices that protects those components and services. Protected resources are the source and destination addresses of a policy-based VPN.
Protected resources consist of three elements:

- **IP Address**—The address represents the computer, network, or range of addresses to be considered part of this protected resource. The Address can be an individual host, a network, or an address group.

- **Network Service**—Services are the protocols (HTTP, FTP) that communicate over a network. The service can be an individual service or a service group.

- **Traffic Direction**—Traffic direction is determined by the IP address that initiates the connection:
  - Client connections are outgoing (outbound) from the protected network.
  - Server connections are incoming (inbound) to the protected network.
  - To protect incoming and outgoing traffic, select Both.

- **Security Device**—The device that protects the network component and server. If the resource can be reached through more than one device, add multiple devices to the resource. When you add a protected resource to a VPN, the devices in the protected resource are included in the VPN.

Each protected resource represents an address or a range of addresses on your network. Each resource also can specify a service (such as FTP or NSF). Therefore, the protected resource is the destination for all traffic using the selected service to the selected address.
Configuring Protected Resources

Chapter 8: Configuring Objects

You can have more than one protected resource for a single address or range of addresses. That way you can individually manage different services traffic to the same destination separately.

Creating Protected Resources

To add a protected resource object:

1. In the navigation tree, select VPN Manager > Protected Resources. In the main display area, click the Add icon to display the Protected Resource dialog box.

2. Enter a name for the protected resource.

3. Select the services you want to permit to this resource, such as FTP, HTTP, NFS, and so on. Select Any to permit all services.

4. Select the initiator of the permitted service: Server, a Client, or Both.

5. Select the address object or address group for the resource.

6. Add the security device through which traffic can reach the protected resource:
   a. In the Security Gateway area, click the Add icon to display the Security Gateway dialog box.
   b. Select security device or device group
   c. Select the security zone on the security device that contains the address objects.
   d. Click OK to add the security gateway to the protected resource.

You can add multiple security gateways to provide redundant access for the protected resource.

Editing Protected Resources

You can edit protected resources to accommodate changes in your network:

- If you make changes to a protected resource object that is used in a VPN, NetScreen-Security Manager automatically generates new configuration and propagates your changes to all affected security devices.

- If you change the security device that protects a resource, NetScreen-Security Manager removes the previous security device from all affected VPNs and adds the new security device. However, NetScreen-Security Manager does not configure the VPN topology for the new security device—you must reconfigure the topology to include the new device manually.
Configuring IKE Proposals

In an AutoKey IKE VPN, you can use the Internet Key Exchange (IKE) protocol to generate and distribute encryption keys and authentication algorithms to all VPN nodes. IKE automatically generates new encryption keys for the traffic on the network, and automatically replaces those keys when they expire. Because IKE generates keys automatically, you can give each key a short life span, making it expire before it can be broken. By also exchanging authentication algorithms, IKE can confirm that the communication in the VPN tunnel is secure.

Because all security parameters are dynamically assigned, VPN nodes must negotiate the exact set of security parameters that will be used to send and receive data to other VPN nodes. To enable negotiations, each VPN node contains a list of proposals; each proposal is a set of encryption keys and authentication algorithms. When a VPN node attempts to send data through the VPN tunnel, IKE compares the proposals from each VPN node and selects a proposal that is common to both nodes. If IKE cannot find a proposal that exists on both nodes, the connection is not established.

IKE negotiations include two phases:

- In Phase 1, two members establish a secure and authenticated communication channel.
- In Phase 2, two members negotiate Security Associations for services (such as IPSec) that require key material and/or parameters.

By default, NetScreen-Security Manager includes several common IKE phase 1 and phase 2 proposals. To view these proposals, open VPN Manager and select IKE Phase 1 Proposals or IKE Phase 2 Proposals.

Creating Custom IKE Phase 1 Proposals

Create a custom proposal for a specific combination of authentication and encryption that is not available in the predefined proposals, or to match the name of proposals on a non-security device.

To create a custom IKE Phase 1 proposal, select Custom IKE Phase 1 and click the Add icon. Enter a name and choose a color for the object, then configure the following settings:

- Authentication Method—Select the authentication method.
  - Preshared Key. Use this option to generate an ephemeral secret and authenticate data using MD5 or SHA hash algorithms against the secret.
  - RSA Certificate.
  - DSA Certificate.
- Diffie-Hellman Group—The Diffie-Hellman group provides asymmetric encryption to encrypt the keys needed to decrypt the data. The larger the modulus of the group, the more secure the generated key is—and the more time it takes to generate the key. Select the group that meets your security requirements and user needs.
Group 1. Uses a 768-bit modulus.
Group 2. Uses a 1024-bit modulus.
Group 5. Uses a 1536-bit modulus.

Encryption Algorithm—Select the algorithm that meets your security requirements:
- DES-CBC
- 3DES-CBC
- AES-CBC (128 Bits)
- AES-CBC (192 Bits)
- AES-CBC (256 Bits)

Hash Algorithm—Select the algorithm that meets your security requirements.
- MD5. Authenticate data using Message Digest version 5.
- SHA-1. Authenticate data with Secure Hash Algorithm-1.

Lifetime—Enter the number of seconds before the key is regenerated. The default value is 28800 seconds (8 hours).

Click OK to add the custom IKE object to the management system.

Creating Custom IKE Phase2 Proposals
Create a custom proposals for a specific combination of authentication and encryption that is not available in the predefined proposals, or to match the name of proposals on a non-security device.

To create a custom IKE Phase2 proposal, select Custom IKE Phase2 and click the Add icon. Enter a name and choose a color for the object, then configure the following settings:

Perfect Forward Secrecy—PFS ensures that a single key permits access to data protected by that single key. The key used to protect transmission of data and the material used to create that key are used only once and are not used to derive additional keys. Select the DH group to encrypt the key:
- No Perfect Forward Secrecy.
- Diffie-Hellman Group 1.
- Diffie-Hellman Group 2.

NOTE: Security devices use hardware encryption for DES and 3DES and use software encryption for AES.
- Diffie-Hellman Group 3.

- Lifetime (Seconds)—Enter the number of seconds before the key is regenerated. The default value is 3600 seconds (8 hours).

- Lifesize (KB)—Enter the number of bytes permitted through the connection before the key is regenerated. A value of 0 (the default) means no limit.

- Encryption (ESP) or Authentication (AH) Algorithm.
  
  - Select ESP to configure encryption and authentication, then select the desired algorithms.
  
  - Select AH to configure authentication only, then select the desired algorithm.

**NOTE:** We strongly recommend that you do not use null AH with ESP.

Click OK to add the custom IKE object to the management system.
Chapter 9
Configuring Security Policies

Firewall rules define access to your network, including permitted services, users, and time periods. You can also use firewall rules to control the shape of your network traffic as it passes through the firewall or to log specific network events. Multicast rules permit multicast control traffic, such as IGMP or PIM-SM messages, to cross Juniper Networks security devices. Multicast rules permit multicast control traffic only; to permit data traffic (both unicast and multicast) to pass between zones, you must configure firewall rules.

This chapter contains the following sections:

- About Security Policies on page 320
- Creating a Security Policy on page 326
- Configuring Firewall Rules on page 330
- Configuring Multicast Rules on page 347
- Configuring Antivirus Rules on page 349
- Configuring Antispam Rules on page 350
- Configuring IDP Rules on page 350
- Configuring Exempt Rules on page 364
- Configuring Backdoor Rules on page 367
- Configuring SYN Protector Rules on page 372
- Configuring Traffic Anomalies Rules on page 376
- Configuring Network Honeypot Rules on page 382
- Installing Security Policies on page 385
- Managing Rules and Policies on page 391
- Pre/Post Rules on page 400
- Polymorphic Objects on page 408
Because all incoming and outgoing network traffic passes through your firewall, it is the ideal location to control the traffic flowing on your network. Creating Security Policies enables you to define what type of traffic should be permitted on your network, as well as how that traffic is treated while inside. A Security Policy can contain firewall rules (in the Zone and Global rulebases), multicast rules (in the Multicast rulebase), and IDP rules (in the IDP, Exempt, Backdoor Detection, SYN Protector, Traffic Anomalies, and Network Honeypot rulebases).

**About Security Policies**


Using the NetScreen-Security Manager UI, you can configure rules in up to six rulebases (Zone, Global, Multicast, IDP, Exempt, Backdoor Detection, SYN Protector, Traffic Anomalies, and Network Honeypot) for each Security Policy. Each rule in a rulebase is a row; you configure the columns in the row to define the rule parameters, such as traffic match conditions, action, and logging requirements. By default, each rulebase displays a subset of available columns for each rule. This mode, known as compact mode, contains columns in which you can configure typical rule parameters. To see additional columns, change the mode of the Security Policy to Expanded: From the menu bar, select View > Expanded Mode. You can set a different mode for each Security Policy.

After you create a Security Policy by building rules in one or more rulebases, you can assign that policy to specific security devices. For information about assigning a policy to a device, see “Assigning a Security Policy to a Device” on page 385.

**NOTE:** In the ScreenOS WebUI and CLI, a Security Policy is a single statement that defines a source, destination, zone, direction, and service. In NetScreen-Security Manager, those same statements are known as rules, and a Security Policy is a collection of rules.

**About Rulebases**

A rulebase is a set of rules that define how the security device handles traffic. NetScreen-Security Manager supports three firewall rulebases and six IDP rulebases, as detailed in the following sections. A Security Policy can contain only one instance of any rulebase type.

By default, the predefined roles System Administrator, Domain Administrator, and IDP Administrator can view and edit all rulebases. The Read-Only System Administrator and Read-Only Domain Administrator can only view rulebases. When creating a custom role, you can include permissions to view or edit individual rulebases.

NetScreen-Security Manager supports the following firewall rulebases:
Zone — 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 and VPN rules and links.

Global — Contains rules that are valid across all zones. Create a firewall rule in the global rulebase when you need to control specific traffic across the entire firewall. The global rulebase can contain only firewall rules.

Multicast — Contains rules that enable IGMP proxy or PIM-SM multicast control traffic between zones.

NetScreen-Security Manager supports two kinds of IDP-capable devices: standalone IDP Sensors, and the ISG family of devices, which can provide firewall and IDP functionality.

NetScreen-Security Manager supports the following IDP rulebases:

- IDP — This rulebase protects your network from attacks by using attack objects to detect known and unknown attacks. Juniper Networks provides predefined attack objects that you can use in IDP rules. You can also configure your own custom attack objects. For more information about IDP attack objects, see “Working with IDP Attack Objects” on page 237.

- Exempt — This rulebase works in conjunction with the IDP rulebase to prevent unnecessary alarms from being generated. You configure rules in this rulebase to exclude known false positives or to exclude a specific source, destination, or source/destination pair from matching an IDP rule. If traffic matches a rule in the IDP rulebase, IDP attempts to match the traffic against the Exempt rulebase before performing the action specified.

- Backdoor Detection — This rulebase protects your network from mechanisms installed on a host computer that facilitates unauthorized access to the system. Attackers who have already compromised a system typically install backdoors (such as Trojans) to make future attacks easier. When attackers send and retrieve information to and from the backdoor program (as when typing commands), they generate interactive traffic that IDP can detect.

- SYN Protector — This rulebase protects your network from SYN-floods by ensuring that the three-way handshake is performed successfully for specified TCP traffic. If you know that your network is vulnerable to a SYN-flood, use the SYN-Protector rulebase to prevent it.

NOTE: Juniper Networks updates predefined attack objects on a regular basis to keep current with newly-discovered attacks. For more information about updating attack objects, “Updating the Attack Object Database” on page 198.

NOTE: If you import the ISG 2000 or ISG 1000 device into NetScreen-Security Manager, the imported device configuration does not include the IDP, Exempt, or Backdoor rulebases.
- **Traffic Anomalies** — This rulebase protects your network from attacks by using traffic flow analysis to identify attacks that occur over multiple connections and sessions (such as scans).

- **Network Honeypot** — This rulebase protects your network by impersonating open ports on existing servers on your network, alerting you to attackers performing port scans and other information-gathering activities.

### Rule Execution Sequence

The rules in all rulebases combine to create a Security Policy. Security devices process and execute firewall and VPN rules in the following order:

1. Zone rulebase
2. Global rulebase
3. Multicast rulebase

Security Devices process and execute IDP rules in the following order:

1. Exempt rulebase
2. IDP rulebase
3. Backdoor rulebase
4. SYN Protector rulebase
5. Traffic Anomalies rulebase
6. Network Honeypot rulebase

### About Rules

A rule is a statement that defines a specific type of network traffic; traffic must meet the rule requirements before it is permitted to pass through the security device. By default, all security devices deny all traffic.

When traffic passes through the security device, the device attempts to match that traffic against its list of rules. Network traffic that matches this list of requirements is considered to “match” the rule, and the device performs the action specified in the rule. If any requirement is not met, the network traffic does not match, and is denied.

Using the NetScreen-Security Manager UI, you can create intrazone firewall rules, global firewall rules, multicast rules, VPN rules, and VPN links for all security devices; for ISG family devices, you can also create IDP rules, exempt rules, and backdoor detection rules. For standalone IDP Sensors, you can create IDP rules, exempt rules, backdoor detection rules, SYN protector rules, traffic anomalies rules, and network honeypot rules. Each Security Policy (all rulebases combined) can contain a maximum of 40,000 rules.
About Firewall Rulebases

You create rules in the firewall rulebases to enable access across your networks by permitting or denying specific network traffic flowing from one zone to another zone. After you have added your security device as a device in NetScreen-Security Manager, you can create rules in the firewall rulebases of your Security Policy.

You can build multiple firewall rules in both firewall rulebases for a single device; these rules combine to create a Security Policy that determines how your security device handles traffic. To simplify your Security Policy, use device groups to build access rules that apply to all your perimeter security devices, then apply the entire policy to the perimeter device group.

Firewall Rules (Zone and Global)

Within a firewall rule, you specify where the traffic is coming from, where it is going, and what service it is using. You can also use firewall rules to authenticate users, monitor network traffic flowing between zones, or set a schedule on a firewall rule that controls the time period that the rule is applied to network traffic.

NOTE: On Juniper Networks vsys devices, rules defined in the root system do not affect rules defined in virtual systems.

When creating firewall rules, consider the type, location, and functionality of each security device in your network. Typically, a single Security Policy for multiple devices works well for devices that perform similar functions, such as perimeter firewalls. However, you might want to create a separate Security Policy per device when the management system contains separate administrators with regional responsibilities, or when you need to troubleshoot a device issue (use one Security Policy per device to enable an admin to troubleshoot on one device without making policy changes on other devices).

A firewall rule must contain the following elements:

- **Direction**—The direction that the traffic flows between two zones; all traffic flows from a source zone to a destination zone. You can select any zone for source or destination; however, the zones must be valid for the security devices you select in the Install On column of the rule. You can also use zone exceptions to specify unique to and from zones for each device.

- **Source address**—The address that initiates the traffic.

- **Destination address**—The address that receives the traffic.

- **Service**—The application-level protocol that the traffic uses to transmit data.

- **Action**—The action the security device performs when it receives traffic that matches the direction, source, destination, and service.

- **Install On**—The security device on which the firewall rule is installed. You can install the same rule on multiple devices.

To begin configuring firewall rules for your managed devices, see “Configuring Firewall Rules” on page 330.
VPN Links and Rules

The rules for your rule-based VPNs appear in the Zone rulebase.

- Use VPN Links for VPNs created in VPN Manager—By default, VPN Manager autogenerated rules are implicitly executed as the first rule in the Zone rulebase, even though they do not appear. Because VPN Manager autogenerates the access rules for the VPN, you do not need to manually create them in the rulebase itself. However, to specify the exact location of the autogenerated rules in your rulebase, you can add a VPN link anywhere in the Zone rulebase.

- Use VPN Rules for VPNs created manually—If you did not use VPN Manager to create a rule-based VPN, you must manually add the VPN rules to create the VPN tunnel. You can place VPN rules anywhere in the Zone rulebase.

Because route-based VPNs are on always-on connection between two or more termination points, you do not need VPN rules to create the routing-based VPN tunnel. However, you might want to create access rules to control the flow of traffic in a routing-based VPN tunnel. For information about adding VPN links or VPN rules, see Chapter 10 “Configuring VPNs”.

NOTE: VPN rules are not validated by rule validation. Only firewall rules are validated by rule validation.

About Rule Groups

A rule group is a user-defined grouping of rules within the Zone rulebase. Combining rules into a rule group can help you better manage rules. For example, you might want to combine your VPN rules in a single rule group, or combine all rules that manage traffic from a specific interface on the security device.

You can add, edit, and delete rule groups; however, deleting a rule group also deletes all rules within that group. You can create multiple rule groups (40,000 rules max in a Security Policy). NetScreen-Security Manager supports one level of rule groups; you cannot create a rule group within a rule group.

NOTE: You can create rule groups only in the Zone rulebase; the Global, Multicast, IDP, Exempt, and Backdoor Detection rulebases do not support rule groups.

For information about rule groups, “Using Rule Groups” on page 395.

About the Multicast Rulebase

By default, security devices do not permit multicast control traffic such as IGMP or PIM-SM messages. If you run IGMP proxy or PIM-SM on your network, you must configure rules in the Multicast rulebase to explicitly permit multicast control traffic between zones.

You can also configure multicast rules to translate multicast addresses. For example, to translate a multicast group address in an internal zone to a different address on the outgoing interface, specify both the original multicast address and the translated multicast group address in a multicast rule.
When you create a multicast rule, you must specify the following:

- **Source zone**—The zone from which traffic initiates.
- **Destination zone**—The zone to which traffic is sent.
- **Multicast group**—The multicast group or access list that specifies the multicast groups for which you want the security device to permit multicast traffic.

Multicast rules control the flow of multicast control traffic only. To permit data traffic (both unicast and multicast) to pass between zones, you must configure rules in a firewall rulebase.

**NOTE:** You cannot create rule groups within the Global or Multicast rulebases.

To begin configuring multicast rules for your managed devices, see “Configuring Multicast Rules” on page 347.

**About IDP Rulebases on ISG Family devices**

For IDP-capable security devices, such as the ISG family running ScreenOS 5.0.0-IDP1, you can enable IDP in a zone or global firewall rule to direct permitted traffic to the IDP rulebases. If you do not enable IDP in a firewall rule for a target device, you can still configure rules in IDP rulebases, but you cannot apply the IDP rules when you update the Security Policy on the target security devices.

When configuring IDP in a firewall rule, consider the following:

- The firewall action must be permit. You cannot enable IDP for traffic that the security device denies or rejects.
- Only traffic that is permitted by the firewall rule is passed to the IDP rulebases. The security device does not forward denied traffic to IDP rulebases.
- You cannot configure DI for the rule; when you install the IDP license on an ISG 2000 or ISG 1000 device running ScreenOS 5.0.0-IDP1, DI is automatically disabled on the device.

**NOTE:** The Attack Profile Settings only apply to the Deep Inspection (DI) feature on security devices.

To enable IDP in a firewall rule, right-click in the Rule Options column for the zone or global firewall rule and select DI Profile/Enable IDP. The DI Profile/Enable IDP dialog box appears (by default, IDP is disabled). Select Enabled to enable IDP for traffic that matches the firewall rule, then select the mode in which you want IDP to operate:

- In inline mode, IDP is directly in the path of traffic on your network and can detect and block attacks. For example, you can deploy the security device with integrated FW/VPN/IDP capabilities between the Internet and an enterprise LAN, WAN, or special zones such as DMZ. This is the default mode.
In inline tap mode, IDP receives a copy of a packet while the original packet is forwarded on the network. IDP examines the copy of the packet and flags any potential problems. IDP’s inspection of packets does not affect the forwarding of the packet on the network.

**About IDP Rulebases on Standalone IDP Sensors**

Standalone IDP Sensors only support IDP-specific rulebases—not firewall rulebases. You do not need to direct traffic to the IDP rulebases; all traffic passing through a standalone IDP Sensor is automatically examined for IDP-related issues.

You must configure the Sensor directly to operate in inline or sensor mode. Refer to the IDP Installer’s Guide for configuration procedures.

In inline mode, a Sensor is directly in the path of traffic on your network and can detect and block attacks. For example, you can deploy the Sensor between the Internet and an enterprise LAN, WAN, or special zones such as DMZ.

In sensor mode, a Sensor receives a copy of a packet while the original packet is forwarded on the network. The Sensor examines the copy of the packet and flags any potential problems. The Sensor’s inspection of packets does not affect the forwarding of the packet on the network.

**Managing Security Policies**

After you have created a Security Policy, you can:

- Modify individual rules in each rulebase, such as changing rule order (determine the order that rules are applied to network traffic by placing the rules in the desired sequential order), disabling a rule, negating source or destination addresses (ScreenOS 5.x devices only), and so on.

- Validate a Security Policy before installing it on your managed devices.

- Merge multiple Security Policies into a single policy for easier management. For example, after importing (or re-importing) devices into the management system, you might want to merge their imported policies into a single policy for all devices.

- Export the policy to an HTML file.

For information about managing your Security Policies, see “Managing Rules and Policies” on page 391.

**Creating a Security Policy**

When creating a Security Policy, consider the following:

- **Objects**—Before creating a Security Policy, you should first use Object Manager to create objects representing your network components, custom services, custom attack objects, and so on. You use these objects when configuring rules within the policy.
If you are running an IDP Sensor, you can use the Profiler to find out what devices are on your network.

- **Pre-Existing Policies**—When creating a new policy, you can use an existing policy as a template. NSM comes with a collection of predefined IDP policies that you can use, or you can use a policy that was created earlier by your organization.

- **Rulebases**—When you initially create a security policy, only the Firewall rulebase and possibly the IDP rulebase appear by default. To create a rule in other rulebases, you must manually add those rulebases to the policy.

The following sections detail these options.

### Configuring Objects for Rules

Objects are reusable logical entities that represent specific settings, configurations, or external pieces of hardware. You can reuse objects in multiple areas in the NSM GUI. Within rules, you use objects to define the source, destination, and service, as well as to specify settings for rule options, such as Web Filtering or attack protection.

For some object types, such as services and IDP attack objects, NetScreen-Security Manager contains a database of predefined objects. If the predefined objects do not meet your networking requirements, you can create custom objects and add them to the object database. For other object types, such as address objects, DI profiles, and Global MIPS, no predefined objects exist; before you can use one of these objects in a rule, you must create the object in Object Manager.

For information about all predefined object settings and creating custom objects, see “Configuring Objects” on page 223.

### Using the Policy Filter Tool

NetScreen-Security Manager provides a Policy Filter tool to filter policy rules-based on one or more filter conditions specified for rule attributes. One filter can contain several filter conditions for different attributes. The filter only applies to the current selected rulebase. The filter results are displayed in the same rulebase. Rules that do not match filter conditions are hidden. In the firewall rulebase, only open rule groups are filtered. When a filter is set and a closed rule group is expanded, only rules that match the filter will be displayed in the group. For information about using the Policy Filter tool, refer to the NetScreen-Security Manager Online Help.

### Filtering the Comment Field

You can use filters for the comments field of your policy. By default, search finds an exact match unless used with a regular expression.

For example, you have two rules with the following two comments: `test1` and `juniper\ntest1`. If you want to find all the rules that have `test1` in the comments field, you must use a regular expression. If you do not use the regular expression checkbox, the search returns rules with comment `test1` only.
If you want to find all rules that end with the string test1, you can use one of the following regular expressions:

- .*test1|.*\n\ntest1
- (.*|.*\n)\ntest1

**Using a Predefined IDP Policy**

When you create a new IDP Security Policy, you can select from the following predefined policies or use the Policy Creation Wizard (as described in the following section).

For the standalone IDP Sensor and ISG with IDP devices, these policies are a good starting point for many common usage scenarios.

NetScreen-Security Manager includes the following Security Policy templates:

- **all_with_logging**—Includes all Attack Objects and enables packet logging for all rules.
- **all_without_logging**—Includes all Attack Objects but does not enable packet logging.
- **dmz_services**—Protects a typical DMZ environment.
- **dns_server**—Protects DNS services.
- **file_server**—Protects file sharing services, such as SMB, NFS, FTP, and others.
- **getting_started**—Contains very open rules. Useful in controlled lab environments, but should not be deployed on heavy traffic live networks.
- **idp_default**—Contains a good blend of security and performance.
- **Recommended**—Contains only the attack objects tagged as “recommended” by Juniper Networks security team. All rules have their Actions column set to take the recommended action for each attack object. By default, this policy is loaded onto all new IDP Sensors when they are added to NSM via the Add Device Wizard.
- **web_server**—Use this template to protect HTTP servers from remote attacks.

Each Security Policy template contains rules that use the default actions associated with the Attack Object severity and protocol groups. You should customize these templates to work on your network by selecting your own Address Objects as the Destination IP and choosing IDP actions that reflect your security needs.

**Using the Policy Creation Wizard**

This wizard guides you through the security policy creation process. Use the wizard to specify the type of device the policy is for and the level of security you want. You can create a policy containing a zone-based firewall rulebase with one any-any-deny rule and/or an IDP rulebase. All other rulebases are optional and can be added to the policy based on need and access control permissions.
If you are logged in as an IDP Administrator, firewall-only rulebases are not available.

The Security Policy Creation wizard lets you select policies for the following devices:

- **Firewall/VPN**—Select this option to create a new policy containing a zone-based firewall rulebase with one any-any-deny rule. This option has only one set.

- **Stand Alone IDP**—Select this option to create a new policy containing the IDP rulebase.

- **Integrated Security Gateways**—Select this option to create a new policy containing a zone-based firewall rulebase with one any-any-permit IDP enabled rule as well as the IDP rulebase.

---

**NOTE:** If you do not have appropriate access-control permission and you attempt to create a policy, the wizard returns an error message stating that you do not have access to create rulebases.

---

**EXAMPLE: CREATING A STANDALONE IDP SECURITY POLICY**

In this example, you create a standalone IDP security policy that logs all levels of attack (Critical, Major, Minor, Warning, and Info) but drops connections only for critical and major attacks.

1. Click Security Policies, then go to the File menu and select New Policy.
2. Give the policy a name and add comments (optional), then click Next.
3. Select Create New Policy for (the default selection). Uncheck Firewall/VPN Devices and check Stand Alone IDP Devices, then click Next.
4. Select Configure IDP Policy, then click Next.
5. Check the boxes and select Enable Logging for all attack levels. Select Drop Connection for critical and major attacks. Click Next twice to continue.
6. Select the device to which you want to assign this policy, then click Next.
7. Click Finish.

**Adding Rulebases**

Security policies start with a minimum of rules and rulebases. You can add additional rules to the rulebases as needed.

To add a rulebase:

1. In the main navigation tree, select Security Policies, then double-click the policy name in the Security Policies window.
2. Click the Add icon in the upper right corner of the Security Policy window and select Add < name> Rulebase. The rulebase tab appears.
3. To configure a rule in the rulebase, click the Add icon on the left side of the Security Policy window. A default rule appears.

4. To add a new rulebase, click the Add icon in the upper right corner of the Security Policy window, then select the rulebase you want to add from the menu. You cannot add a rulebase more than once, so only rulebases that are not already in the policy are displayed.

The following sections explain how to configure rules in each rulebase.

**Configuring Firewall Rules**

The firewall rulebases enable you to create zone and global firewall rules that control the flow of traffic on your network. You can configure the following settings for a firewall rule:

- Defining Match for Firewall Rules
- Defining Actions For Firewall Rules
- Selecting Devices for Firewall Rules
- Configuring Firewall Rule Options
- Comments For Firewall Rules

For each rule, you must configure the rule parameters for the Match columns. The remaining columns are optional, however, the more specific you can be in defining rule parameters in each column, the more efficient your Security Policy can be when protecting your network.

**Defining Match for Firewall Rules**

A firewall rulebase controls traffic flow on your network, from one network component to another network component. To do this, the firewall must know the path that the traffic takes to reach its destination and the service the traffic uses to get there.

When creating your firewall rules, you must specify the areas in your network that the traffic passes through. These areas include the network components that originate and receive the traffic, and the firewall zones the traffic passes through. For firewall rules:

- The Destination Address, Source Address, Service, and Action are required for all rules in the Zone and Global rulebases.
- The To Zone, From Zone, and service are required for rules in the Zone rulebase.

The following sections detail the Match columns of a firewall rule.
Configuring Source and Destination Zones for Firewall Rules

In the Zone rulebase, you create firewall rules to enable traffic to flow between zones (interzone) or between two interfaces bound to the same zone (intrazone). You must create zones on your security device before you can create a rule for that device. In a single rule:

- You must select a single zone for the source zone and a single zone for the destination zone. These zones must be available on the security devices you will install the policy on.

- You can also select multiple zone exceptions for both source and destination zones. A zone exception includes a specific zone and the device that contains that zone.

- You cannot create a rule that controls traffic between zones shared by vsys devices or by devices in an NSRP configuration.

The Global rulebase does not contain source and destination zone columns. Because global rules permit or deny traffic flow between all zones on the security device, both the source and destination zones are global and so are not displayed.

Configuring Source and Destination Addresses For Firewall Rules

You create firewall rules to enable traffic to flow between two network components. In the NetScreen-Security Manager system, address objects are used to represent the components on your network: hosts, networks, and servers. When you add the address object to the rule, you are assigning it to a security zone on your security device.

You can add predefined Address Objects for the network components that originate and receive the traffic, or configure them as you create a firewall rule to control traffic between those components:

- To predefine an Address Object, see “Configuring Address Objects” on page 227.

- To configure an Address Object as you are configuring the Source and Destination components of a rule, right-click in the Source or Destination column of a rule and select Add Address. Next, click the Add icon at the top of the New Source Addresses or New Destination Addresses dialog box and configure the desired address object. For information about configuring an address objects, see “Configuring Address Objects” on page 227.

- You can add an entire address group or select an individual address object from within the group.

You can also negate all address objects in the source or destination columns of a rule. When the source or destination is negated, NetScreen-Security Manager considers all address objects defined for the current domain except the negated objects as part of the source or destination for that rule. To negate the source or destination, you must have previously added one or more address objects to the source or destination column of a rule.
You can add global MIP and/or VIP objects as the source or destination address in a rule. However:

- When installing the rule on devices running ScreenOS 4.0, you can add multiple MIPs.
- When installing the rule on devices running ScreenOS 5.3, you can add multiple MIPs and VIPs.
- When installing the rule on devices running ScreenOS 5.0 or higher, you can add a single MIP object per rule. To use multiple MIP objects for these devices, you must use a separate rule for each global MIP object.

If you select multiple MIP or VIP objects in the source or destination column of a rule that includes devices running non-ScreenOS 5.3 or higher in the Install On column, a validation message appears, indicating that those devices do not support multiple MIPs or VIPs within a single rule.

**EXAMPLE: SETTING INDIVIDUAL SOURCES AND DESTINATIONS IN RULES**
To control incoming Internet traffic to your trusted network, set the From Zone to Untrust and the To Zone to **Trust**. Set the source address as **any** and the destination to the address object that represents your trusted network. See Figure 69.

![Figure 69: Set Individual Sources and Destinations in a Firewall Rule](image)

To create a broader rule that controls traffic between multiple network components, create Address Object groups and use them in your firewall rules as you would other address objects. However, because security devices running ScreenOS 4.0.x apply firewall rules to each address object separately, using address object groups can quickly decrease the number of available internal logical rules. If you must use address groups for both the source and destination, ensure that these groups are as small and as specific as possible.

**EXAMPLE: SETTING GROUP SOURCES AND DESTINATIONS IN RULES**
To control traffic from your Marketing servers to your Engineering Servers, set the To Zone to Engineering and the From Zone to Marketing. Set the source address as the address group object that represents your Marketing servers, and the destination address to the address group object that represents your Engineering servers. See Figure 70.

![Figure 70: Set Group Sources and Destinations in a Firewall Rule](image)

The more specific you are in defining the source and destination address in a firewall rule, the better your firewall performance will be.
EXAMPLE: NEGATING SOURCES IN RULES
To permit incoming traffic to your Engineering department network from any network except the Sales network, set the From Zone to Untrust and the From Zone to Trust. Set the source address group as the address group that represents Outside Sales network, and the destination address to the address group that represents your Engineering server network. Finally, right-click inside the source address column for the rule and select Negate. See Figure 71.

Figure 71: Negate Source in a Firewall Rule

<table>
<thead>
<tr>
<th>Match</th>
</tr>
</thead>
<tbody>
<tr>
<td>From Zone</td>
</tr>
<tr>
<td>untrust</td>
</tr>
</tbody>
</table>

Configuring Services for Firewall Rules
Services are application layer protocols that define how data is structured as it travels across the network. In NetScreen-Security Manager, Service Objects represent the services running on your network. In a firewall rule, you specify which services are supported by the destination address object.

NOTE: All services rely on a transport layer protocol to transmit data. NetScreen-Security Manager includes services that use TCP, UDP, RPC, and ICMP transport layer protocols.

NetScreen-Security Manager comes with several service objects based on industry-standard services already created for you. You use these predefined service objects in firewall rules to specify the services that traffic can use to traverse your network.

EXAMPLE: SETTING STANDARD SERVICES IN RULES
To control FTP traffic from the Engineering Server in the trust zone to the corporate Web Server in the DMZ zone, select the FTP, HTTP, IMCP ANY, and TELNET service objects. See Figure 72.

Figure 72: Set Standard Services in a Firewall Rule

<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: SETTING CUSTOM SERVICES IN RULES
If you use a non-standard port (8080) for your HTTP services, create an HTTP Service Object on port 8080. Add this Service Object to your firewall rule. NetScreen-Security Manager uses the specified service object, HTTP on port 8080, and considers all connections to TCP/8080 to be HTTP connections. Your rule is similar to the example below:

Figure 73: Set Custom Services in a Firewall Rule

<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.x device, if you use a custom service to relocate an application to a non-standard port, you must also enable the Application option in the Rule Options > Miscellaneous > ScreenOS 5.x devices. For details, see “ScreenOS 5.x and Later Options” on page 340.

Defining Actions For Firewall Rules
You can specify the action that your security device performs against traffic that matches the zones, address objects, and services specified in the firewall rule. You can set different actions for each rule:

- **Permit**—The managed device permits the traffic to pass through the firewall to its destination address.
- **Deny**—The managed device does not permit the traffic to pass through the firewall and drops all associated packets. No notification is returned to the sender.
- **Reject**—The managed device does not permit the traffic to pass through the firewall and drops all associated packets. For TCP and UDP packets, the device returns a notification message to the packet sender:
  - When the device drops a TCP packet, it returns a TCP RST packet to the sender.
  - When the device drops a UDP packet, it returns an ICMP port unreachable error to the sender.

  For non-TCP and non-UDP packets, no notification is returned to the sender.

When you permit traffic, you can also:

- Use logging to monitor suspicious or abnormal uses of permitted traffic (such as excessive Web surfing).
- Use AntiVirus to detect viruses in permitted traffic.
Use Web Profiles to detect and prevent access to malicious or undesirable URLs.

Use DI Profiles to detect and prevent attacks in permitted traffic.

Selecting Devices for Firewall Rules

In the install on column, select the device(s) that receive and use this rule. You can select multiple security devices on which to install the firewall rule. After you have created the Security Policy and assigned it to a device, NetScreen-Security Manager installs the rule only on the devices specified in the Install Column of the rule, enabling you to use a single Security Policy for multiple security devices.

To see the exact rules that are applied to a specific device, in Device Manager, right-click a device and select Policy > View Pending Device Policy.

NOTE: If a device specified in the Install column does not support a specific rule option configured for the rule, you can still install the Security Policy on the device, but the rule option is not enabled for that device. Additionally, during policy validation, a warning appears for each unsupported rule option. For details, see “Validating Security Policies” on page 386.

Configuring Firewall Rule Options

Rule options enable you to configure additional protection mechanisms and other miscellaneous features. You can configure the following rule options:

- Enabling NAT
- Enabling GTP for Firewall Rules
- Configuring Traffic Shaping in a Security Policy
- Enabling Logging and Counting for Firewall Rules
- Miscellaneous
- ID
- Configuring Web Filtering for Firewall Rules
- Configuring Authentication For Firewall Rules
- Configuring AntiVirus For Firewall Rules
- Configuring a DI Profile/Enable IDP For Firewall Rules

To quickly configure all rule options, right-click the Rule Options column and select Configure All Options. The Configure Options dialog box appears; select the option tab you want to configure for the rule.
Enabling NAT
You can configure policy-based network address translation (NAT) for a firewall rule. NAT enables the security device to translate the IP address of incoming or outgoing traffic so that the packets are routeable on the network.

Edit Source NAT
You can configure the security device to translate the source IP address:

- To translate the source IP address using a predefined range of IP addresses, select NAT and choose a Dynamic IP pool (DIP) object. For each matching packet, the device translates the original source address into a IP address selected from the DIP pool.

- To translate the source IP address using the IP address of the outgoing interface on the security device, select Use Interface.

Edit Destination NAT
You can configure security devices running ScreenOS 5.x to translate the destination IP address. Enable Destination NAT and enter the destination IP address you want to translate to.

Other destination NAT options include:

- **Destination Port**—Your security devices can perform one-to-one destination NAT without changing the destination port numbers. However, you can configure the device to map the original destination port number in the segment header to another port number.
  
  - To enable destination port translation, select Destination Port and enter the port number you want to translate to.
  
  - To use the original destination port number, leave the default of None.

- **Upper IP Address**—Your device can also translate the destination IP address to a range of IP addresses. Select the Upper IP Address and enter the upper IP address. The device uses an address shifting mechanism to maintain the relationships among the original range of destination addresses after translating them to the new range of addresses.

Using Device Manager, you can also implement NAT on any device interface in any zone except Untrust. For details, see “NetScreen-Security Manager: Configuring Firewall/VPN Devices”. For information about configuring NAT objects, see “Configuring NAT Objects” on page 308.

Enabling GTP for Firewall Rules
You can use a GTP object in a firewall rule to control how your security devices handle GPRS traffic. To add a GTP object, you must have already configured the object in Object Manager. For details, see “Configuring GTP Objects” on page 275.
Configuring Traffic Shaping in a Security Policy

Traffic shaping enables you to control the amount of bandwidth that is available to the matching network traffic in a rule. You can also define a priority that defines how the security device handles the matching network traffic that exceeds the defined maximum bandwidth. For security devices running ScreenOS 5.3, you can also manage the flow of traffic through the security device by limiting bandwidth at the point of ingress.

You can configure the following traffic shaping parameters:

- **Traffic Shaping Mode**—The traffic shaping mode is automatically determined by the security device, but you can set it to on or off.

- **Bandwidth**—You can control the amount of bandwidth that is available to the matching network traffic. When traffic shaping is enabled, you can configure the minimum, or guaranteed bandwidth allowed, by setting the number of kilobits per second (kbps) using the Guaranteed Bandwidth field. This setting guarantees that this minimum amount of throughput is allowed to pass through the security device. In a similar manner, you can set the maximum bandwidth allowed using the Maximum Bandwidth field. For matching traffic that falls between the guaranteed and maximum settings, the security device passes traffic based on the priority setting.

- **Priority**—You can set a priority for each firewall rule in your Security Policy. Your security device passes permitted traffic according to the priority level specified in the matching rule. The higher the priority level of the rule, the faster the matching traffic for that rule passes. You can configure the mappings of eight priority levels to the first three bits in the DiffServ field or to the IP precedence field in the ToS byte in the IP packet header. By default, the highest priority (priority 0) on the security device maps to 1 1 1 in the IP precedence field. The lowest priority (priority 7) maps to 0 0 0 in the IP precedence field.

- **DSCP Class Selector**—NetScreen-Security Manager uses the Differentiated Services Code Point (DSCP) mechanism to set priority levels. Using DSCP, you can mark traffic at a position within a hierarchy of priority. You can map eight priority levels to the DiffServ system: Priority 0 is the highest priority, and priority 7 is the lowest priority. Each priority level maps to a specific set of bits in the DiffServ field or the IP precedence field in the ToS byte of the IP packet header. The class selector controls the number of bits affected in the DiffServ field. By default, the priority levels affect only the first three bits in the eight bit DiffServ field. The remaining bits are untouched, but can be altered by an upstream router, which might change the IP priority preference.

**NOTE:** We recommend that you set the maximum bandwidth to greater than 10 kbps. When the bandwidth is set to less than 10 kbps, the security device might drop packets or the source address might attempt to resend the traffic repeatedly.

For security devices running ScreenOS 5.3, you can also manage the flow of traffic through the security device by limiting bandwidth at the point of ingress. To configure the maximum amount of traffic allowed at the interface ingress, you need to first enable Use Policing Bandwidth, and then set the number of kbps using the Policing Bandwidth field. This setting allows you to manage the maximum amount of traffic allowed to pass through the ingress interface.
When the DSCP class selector is enabled, the class selector zeroes the remaining five bits in the DiffServ field, which prevents upstream routers from altering priority levels.

For information about changing the default mappings between priority levels and the DiffServ system, see “NetScreen-Security Manager: Configuring Firewall/VPN Devices”.

---

**NOTE:** You can only apply traffic shaping to rules whose destination zone has a single interface bound to it. Security zones that contain subinterfaces or that contain more than one physical interface do not support traffic shaping.

---

For more information about Traffic Shaping, refer to the NetScreen Concepts & Examples ScreenOS Reference Guide.

---

Enabling Logging and Counting for Firewall Rules

A good Security Policy generates enough log entries to fully document only the important security events on your network. However, if you need to keep a record of all log entries for archiving and accountability, you can design your rule to log every security event. For critical events, you might even want to be notified immediately by email or set an alert to appear in the log entry.

Log entries appear in real-time in the Log Viewer and are also used in the Log Investigator for cross-tabulation of security events. Your goal is to fine-tune the notifications in your Security Policy to your individual security needs.

---

**Configuring Logging and Alerts**

To log an event for a rule, enable logging. Each time your security device matches network traffic to the rule, the device creates a traffic log entry that describes that event and NetScreen-Security Manager displays the traffic log entry in the Log Viewer. You can enable logging when a session is initialized, closed or both on a security device. For a list of possible traffic log entries, see “Traffic Log Entries” on page 776.

Depending on your security needs, you might want NetScreen-Security Manager to provide additional notification when a rule is matched, such as an alert in the log entry. An alert is a notification icon ( ) that appears in a log entry in the Log Viewer. When you enable alerts in your firewall rule and traffic matches that rule, the device generates a traffic log entry that includes an alert. Alerts can help you quickly identify specific network traffic, such as critical severity attacks.

You must enable logging before you can enable alerts.

---

**Configuring Counting and Alarms**

Counting and alarms work together to help you track the amount of traffic that is matching your firewall rule. Counting enables the device to count the number of bytes in network traffic that matches the firewall rule. Using this data, the device can then generate alarms that notify you when the matching network traffic falls outside your predefined byte range.
To set an alarm, enable counting and specify the minimum and maximum byte thresholds for matching network traffic. You can specify a predefined number of bytes per second, number of Kilobytes per minute, or both. Each time your security device detects network traffic that exceeds the alarm threshold in the rule, the device generates an alarm log entry for that describes that event and displays it in the Log Viewer. For a list of possible alarm log entries, see “Alarm Log Entries” on page 707.

You must enable counting before you can enable alarms. Although you can enable counting without also enabling alarms, NetScreen-Security Manager does not use the counting data except to trigger alarms. If you do not intend to use alarms, you should leave counting disabled. Additionally, because counting can impact performance during heavy traffic periods, you should enable counting and alarms only for firewall rules that detect important activity.

### Configuring Log Actions

Use the Log Actions tab that appears when you select Log/Count in the Rule Options column to configure the following actions to occur when a log is generated from a specific rule:

- **Sending SNMP Trap**—Selecting this option directs the system to output logs to an SNMP server in SNMP format.
- **Sending Syslog Messages**—Selecting this option directs the system to output logs to a syslog server in syslog format.
- **Writing CSV files**—Selecting this option and specifying a filename directs the system to output logs using in CSV format.
- **Writing XML Files**—Selecting this option and specifying a filename directs the system to output logs using XML.
- **Sending Email**—Selecting this option directs the system to output logs to an email address in SMTP format. You must specify the recipient email address(es) that receives the exported log records.
- **Running Scripts**—Selecting this option directs the system to execute a script and report output status. You must specify the script that receives the exported log records (script must be located in the /usr/netscreen/DevSvr/lib/scripts/ directory). In the event that the script fails, you can also configure the system to retry or skip running the script again.

You can configure parameters for forwarding logs to SNMP, Syslog, Email, CSV and XML in the Action Parameters node of the Action Manager.

### Miscellaneous

The following sections detail the Miscellaneous rule options.
Schedule
To control the time period that your security device applies the rule to your network traffic, you can define a schedule for the rule. If you define a schedule, the security device applies the rule to your network traffic only during the time period specified in the schedule; if you do not specify a schedule, the rule is always applied to your network traffic.

In NetScreen-Security Manager, schedules are represented by Schedule Objects. Before you can define a schedule for a rule, you must create a Schedule Object that describes a time period. The Schedule Object defines the start time and date, end time and date, and frequency (recurring or one-time) of the time period. For more information about creating Schedule Objects, see “Configuring Schedule Objects” on page 232.

You can use schedules to control the flow of network traffic at a time-sensitive level, and also enhance your network security.

Example: Setting Schedule Objects in Rules
To prevent employees from downloading large files during business hours, set the Service Object to FTP, the Action to deny, and configure traffic shaping to limit bandwidth. Using the Object Manager, create a Schedule Object called Business Day that describes the time period of 9:00am to 7:00pm, M-F, recurring weekly. Right-click the schedule column in the rule and select the Business Day schedule object.

HA Session Backup
NetScreen-5XT and NetScreen-5GT security devices can disable active firewall rules that permit traffic if the session switches over to the modem link. This feature is ON by default.

ScreenOS 5.x and Later Options
For security devices running ScreenOS 5.x and later, you can configure additional rule options.

- Application—You can configure the security device to handle the service for the firewall rule as a known Layer 4 protocol service. If you are using application relocation (using a nonstandard port to handle an application service), enable this option to ensure that the security device correctly checks traffic.

ID
The rule ID is a number that uniquely identifies a rule within the rulebase and Security Policy. After you install a rule as part of a Security Policy on a security device, you can view that rule by logging in locally to the device with the WebUI or CLI where the rule appears as an individual policy. The individual policy on the device has the same ID as the rule in the management system, which helps you keep track of which rules are on which devices.

You can configure a rule ID for any Zone-based firewall rule or VPN rule:

- For new rules, NetScreen-Security Manager automatically assigns a unique ID to that rule. You can change this ID, if desired, or leave the ID number.
For rules that are already installed on a device, NetScreen-Security Manager has already created a unique ID for the rule. You can change this predefined ID if desired, to an ID number, or leave the ID set to “none”, which preserves the autogenerated ID number.

**NOTE:** When the ID is set to “none”, NetScreen-Security Manager uses a hashing algorithm on the source zone, destination zone, source address, destination address, and service fields for the rule to generate a unique ID.

For VPN rules that are automatically created by VPN Manager, NetScreen-Security Manager creates a unique ID for each VPN rule. You can change this predefined ID, if desired, to a ID number, or leave the predefined ID set to “none”, which preserves the autogenerated ID number.

When you copy and paste a rule within a rulebase, NetScreen-Security Manager automatically creates a new unique ID for the pasted rule.

You are not required to set a ID for a rule.

**Configuring Web Filtering for Firewall Rules**

After you create a Web Filtering profile [refer to Chapter 7, Configuring Web Filtering (Integrated)], and you have enabled Web Filtering on your device (refer to Chapter 4, Configuring Devices), you need to bind it to your firewall rule. You need to select one of the following options:

- **Web Filtering Through SurfControl SCFP/WebSense (Redirect)**—With this option, the security devices sends the first HTTP request in a TCP connection to either a Websense server or a SurfControl server, enabling you to block or permit access to different web sites based on their URLs, domain names, and IP addresses.

- **Web Filtering Through SurfControl CPA (Integrated)**—With this option you permit or block access to a requested website by binding the default ns-profile or custom profile you created to a firewall rule.

When a profile is bound to the firewall rule, the security device matches the URL in the incoming HTTP request to the categories in the profile in the following sequence:

- Black List
- White List
- Custom URL Lists
- Predefined Web categories

If no custom profile is bound to the firewall rule, the security device uses the default profile `ns-profile`. If the security device does not find the category of the requested URL, then it performs the default action, to permit access to the URL (unless otherwise configured).
EXAMPLE: SETTING A WEB FILTERING PROFILE IN A RULE
In this example, you will bind the predefined Web Filtering profile to a firewall rule.

1. Click Security Policies in the navigation tree. Select the device you want to bind to the Web filter profile.

2. In the Zone based Firewall Rules main display area, right-click under Rule Options. A pull-down menu appears.

3. Select Web Filtering.

4. In the Edit Web filter dialog box, click Enable.


6. Select the profile ns_profile to bind to the firewall rule.

   NOTE: You can only bind one Web Filtering profile to a firewall rule.

   Figure 74: Configure Web Filtering in a Firewall Rule

7. Click OK.
Configuring Authentication For Firewall Rules

You can authenticate the identity of the user who is generating the network traffic. When you enable authentication in the rule, the user must authenticate future network traffic by supplying a user name and password in an initial, separate HTTP, FTP, or Telnet connection. If the user fails to authenticate using one of these services or provides incorrect credentials, the authentication requirement for the rule is not met and the network traffic is denied. (Typically, when you enable authentication, you also use the permit action.)

NOTE: You cannot enable authentication for a rule that includes the DNS/53 Service Object.

Configuring Authentication

Authentication enables you to control which RAS users can connect to the protected network and how they can connect. When you select an authentication server, you must also configure the users that authentication server authenticates.

Select the authentication mechanism:

- **No Authentication**—Use this option to enable the specified RAS users to connect without authentication.
- **Authentication**—Use for RAS users that use HTTP, FTP, or Telnet services to connect to the protected network.
- **Web Authentication**—Use for RAS users using HTTP to connect to the protected network.
- **Infranet Authentication**—Use this option to enable specified RAS users to connect using a Juniper Networks Infranet Controller.

Configuring Users

RAS users are represented by User Objects. Before you can authenticate a user in a firewall rule, you must create a User Object that defines the user name, user password, and the authentication location (local or external). For Authentication and Web Authentication, configure the users:

- **User**—Select the User object that represents the user you want to authenticate.
- **User Group**—Select the User Group object that represents the users you want to authenticate.
- **Group Expression**—Select the Group Expression object.
- **Allow Any**—Use this option to authenticate any user or user group.

To authenticate RAS users with Authentication, you must include HTTP, FTP, or Telnet service objects in the Service column of the rule. You can include other services as well, or select any to specify all services. To make a connection to the destination IP address in the rule, the RAS user first initiates an HTTP, FTP, or Telnet connection to the destination address; the security device intercepts the request packet and responds with a login prompt for user credentials.

NOTE: You cannot enable authentication for a rule that includes the DNS/53 Service Object.
If the destination address is a subnet, the remote user must authenticate for each IP address in that subnet.

If the source address supports multiple remote user accounts (such as a Unix host running Telnet) OR is located behind a NAT device that uses a single IP address for all NAT assignments, only the first remote user from that source address must initiate and authenticate an HTTP, FTP, or Telnet connection. All subsequent remote users from that source address do not need to authenticate, and can pass matching network traffic to the destination address.

To authentication RAS users with Web Authentication, you must include HTTP service object in the Service column of the rule. To make a connection to the destination address in the rule, the RAS user first initiates an HTTP connection to the Web Authentication server. The security device responds with a login prompt for user credentials.

For more information about User Objects, see “Configuring User Objects” on page 298.

Configuring AntiVirus For Firewall Rules
To configure AntiVirus protection for a firewall rule:

- **None**—No AntiVirus protection enabled.
- **Use External AV Server**—Uses an external antivirus scanner. Select an external policy object that defines an external scanner.
- **Use Scan Manager**—Scan Manager is an embedded scanning engine. To use Scan Manager, the security device you install the policy on must be a NetScreen-5GT or NetScreen-Hardware Security Client device running ScreenOS 5.0 - 5.2. If you install a policy that uses Scan Manager on a different device, the device executes and processes traffic according to the rule, but does not detect viruses using the embedded scanning engine.
- **Use Scan Manager with Profile**—Scan Manager is an embedded scanning engine. This setting tells the device to use the global profile specified. This setting only works for devices running ScreenOS 5.3.
- **Use ICAP Profile**—ICAP is a method of redirecting traffic to an ICAP-capable server running AV software. This feature is available on devices running ScreenOS 5.4 and higher.

Configuring a DI Profile/ Enable IDP For Firewall Rules
Use the DI Profile/Enable IDP rule options to configure Deep Inspection (DI) or Intrusion Detection and Prevention (IDP) functionality within the rule.

**NOTE:** This function applies to firewall and ISG devices only. Standalone IDP devices do not use firewall rules.
Configuring Firewall Rules

Chapter 9: Configuring Security Policies

Configuring DI Profile for a Rule

Security devices running ScreenOS 5.x include Deep Inspection attack protection that can detect malicious network traffic at the application level. To configure attack protection, select a DI Profile object in your firewall rule to detect intrusion attempts within permitted traffic.

Attacks are specific patterns of malicious activity within a network connection, and an attack object uses selected sections of the attack pattern to detect the attack itself. NetScreen-Security Manager contains a database of predefined attack objects that detect known and unknown attacks against your network. You can use these predefined attack objects (and your own custom attack objects) to create a DI Profile object, which you then use in a firewall rule. When configuring a DI Profile, you can also define the action that the device performs against those attacks when detected in permitted traffic. For information about creating a DI Profile object, see “Creating DI Profiles” on page 235.

You can configure one DI Profile for each rule. When the device detects a match between the permitted network traffic and an attack object within the selected DI Profile, the device generates an attack log entry.

To use a DI Profile:

- The firewall action must be permit. You cannot detect attacks in traffic that the device denies or rejects.
- The security device you install the policy on must be running ScreenOS 5.x. If you install a policy that contains a DI Profile on a ScreenOS 4.0.x device, the device executes and processes traffic according to the rule, but does not detect application-level attacks.

For a list of possible attack log entries, see “Deep Inspection Alarm Log Entries” on page 708.

Configuring IDP for a Firewall Rule

When configuring rule for an IDP-capable device, such as the ISG 2000 or ISG 1000 security device running ScreenOS 5.0(IDP1, you can enable IDP and select an IDP mode in the DI Profile/Enable IDP rule options. Enabling IDP directs the security device to pass all traffic permitted by the firewall rule to the IDP rulebase.

NOTE: DI and IDP are mutually exclusive. When you install the IDP license key on a security device, DI is automatically disabled.

When configuring the firewall rule, consider the following:

- Traffic that is denied by a firewall rule cannot be passed to IDP rules. To enable IDP in a firewall rule, the action must be permit.
For firewall rules that pass traffic to the IDP rulebases, the Install On column must include IDP-capable devices only.

To forward traffic to the IDP rulebases, enable IDP and select one of the following modes:

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

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

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

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

**Comments For Firewall Rules**

The Comments column of a rule contains the rule title, which is also the ScreenOS policy name (the name of the policy when viewing the device configuration using the WebUI).

You can also enter comments in the Comment Field, if desired.

**Configuring Multicast Rules**

A multicast rule is a statement that defines a specific type of multicast control traffic. When multicast control traffic passes through a security device, the device attempts to match that traffic against its list of rules. If a rule is matched, the device permits the traffic to pass through.

On security devices, you secure multicast control traffic using access lists. First, you create an access list, which defines one of the following:

- The multicast groups a host can join.
- The sources from which traffic can be received.

After creating an access list, you reference these access lists in a multicast rule in the Security Policy for the device.

**Configuring Source and Destination Zones**

In the Multicast rulebase, you create rules to enable multicast control traffic to flow between zones. You must create zones on your security device before you can create a rule for that device. In a single rule:
You must select a single zone for the source zone and a single zone for the destination zone. These zones must be available on the security devices on which you install the policy.

You can also select multiple zone exceptions for both source and destination zones. A zone exception includes a specific zone and the device that contains that zone.

**Configuring Source and Destination Groups**

When you create a multicast rule, specify the multicast groups for which you want to permit multicast traffic using one of the following methods:

- Specify a multicast group IP address, and optionally, the multicast group address on the outgoing interface
- Specify the access list that identifies the permitted multicast groups
- Select “any” to accept traffic for all multicast groups

**Configuring Rule Options**

Rule options enable you to specify the type of multicast control traffic to which this rule applies and whether the rule is bidirectional.

A rule can apply to either IGMP messages or PIM-SM messages:

- When running IGMP proxy on the security device, configure a rule that permits IGMP messages to flow between zones.
- When running PIM-SIM on the security device, configure a rule that permits PIM-SM messages.

**EXAMPLE: CREATING A MULTICAST RULE**

In this example, you define a multicast rule that permits IGMP messages from the Trust zone to the Untrust zone. You specify the original multicast group address object and a different destination multicast group object.

1. In the main navigation tree, select Object Manager > Address Objects.
2. In the main display area, click the Add icon and select Multicast Group. In the New Multicast Group dialog box, configure the following then click OK:
   - For Name, enter mcast1.
   - For Color, select green.
   - For IP Address, enter 232.1.1.1.
   - For Netmask, enter 32.
3. In the main display area, click the Add icon and select Multicast Group. In the New Multicast Group dialog box, configure the following then click OK:
   - For Name, enter mcast2.
For Color, select red.

For IP Address, enter 232.1.1.2.

For Netmask, enter 32.

4. In the main navigation tree, select Security Policies, then create a new multicast rule in the Multicast rulebase of a new or existing Security Policy.

5. Right-click in the Source Group column and select Configure Source/Destination. Configure as shown below:

Figure 75: Configure Source/Destination for Multicast Rule

<table>
<thead>
<tr>
<th>No.</th>
<th>Match</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>From Zone</td>
<td>Source Group</td>
</tr>
<tr>
<td>1</td>
<td>trust</td>
<td>mcast1</td>
</tr>
</tbody>
</table>

Configuring Antivirus Rules

Antivirus settings are stored in a profile. To see how to create an antivirus profile, see Configuring AntiVirus Objects on page 265.

To assign an antivirus profile to a policy, do the following:

1. Double-click the Rule Options cell in a rule.

2. In the Configure Options dialog, click the Antivirus tab.

3. Select an Antivirus option:

   - **None**—Turns off antivirus scanning for that rule.
   - **Use External AV Server**—Indicates that you want to use an External AV Server. You must select the external AV server you wish to use. To configure external AV servers, see Configuring External AV Profiles on page 265.
   - **Use Scan Manager**—Tells the device to use the settings on the device, instead of a profile. Necessary for ScreenOS 5.0-5.2.
- **Use Scan Manager with Profile**—Tells the device to use the indicated antivirus profile. Necessary for ScreenOS 5.3 and higher. To set up an internal antivirus profile, see Configuring Internal AV Profiles on page 266.

- **Use ICAP Profile**—Tells the device to use the indicted ICAP AV profile. Available with ScreenOS 5.4 and higher.

4. Click OK.

### Configuring Antispam Rules

Antispam settings are stored in profiles. Initially, Netscreen-Security Manager will have only one antispam profile available: ns-profile.

To assign an antispam profile to a policy, do the following:

1. Double-click the Rule Options cell in a rule.
2. In the Configure Options dialog, click the Antispam tab.
3. Check the Enable Antispam profile checkbox.
4. Select ns-profile in the Profile Name pull-down menu.
5. Click OK.

### Configuring IDP Rules

The IDP rulebase protects your network from attacks by using attack objects to identify malicious activity and take action. Creating an IDP rule involves the following steps:

- **Defining Match for Firewall Rules** (does not apply to rulebases for standalone IDP Sensors) —The type of network traffic you want IDP to monitor for attacks, such as source/destination zones, source/destination address objects, and the application layer protocols (services) supported by the destination address object. You can also negate zones, address objects, or services.

  Standalone IDP Sensors do not use firewall rules.

- **Configuring Terminal IDP Rules**—By default, rules in the IDP rulebase are non-terminal, meaning that IDP examines all rules in the rulebase and all matches are executed. You can specify that a rule is terminal; if IDP encounters a match for the source, destination, and service specified in a terminal rule, it does not examine any subsequent rules for that connection. Note that the traffic does not need to match the attacks specified in the terminal rule. Terminal rules should appear near the top of the rulebase, before other rules that would match the same traffic. Use caution when specifying terminal rules.
- **Configuring Attack Objects in IDP Rules**—The attacks you want IDP to match in the monitored network traffic. Each attack is defined as an attack object, which represents a known pattern of attack. Whenever this known pattern of attack is encountered in the monitored network traffic, the attack object is matched. You can add attack objects by category, operating system, severity, or individually.

- **Configuring Actions**—The action you want IDP to take when the monitored traffic matches the rule's attack objects. You can specify the action you want the security device to perform against the current connection (see “Defining Actions For IDP Rules” on page 356) and future connections from the same source IP address (see “Choosing an IP Action” on page 359).

- **Configuring Notification in IDP Rules**—Disable or enable logging for the IDP rule.

The following sections detail each step.

**Defining Match For IDP Rules**

When creating your IDP rules, you must specify the type of network traffic that you want IDP to monitor for attacks. These characteristics include the network components that originate and receive the traffic, and the firewall zones the traffic passes through.

The Match columns From Zone, Source, To Zone, Destination, and Service are required for all rules in the IDP rulebase. The Terminate Match selection allows you to designate a rule as terminal; if IDP encounters a match for the other Match columns in a terminal rule, no other rules in the rulebase are examined. The matching traffic does not need to match the attacks specified in a terminal rule. (For more information on terminal rules, see “Configuring Terminal IDP Rules” on page 355.

The following sections detail the Match columns of an IDP rule.

**Configuring Source & Destination Zones for IDP Rules** *(Does not apply to Standalone IDP Sensor rulebases)*

You can select multiple zones for the source and destination, however these zones must be available on the security devices on which you will install the policy. You can specify “any” for the source or destination zones to monitor network traffic originating or destined for any zone.

For standalone IDP rulebases, the Zones are always set to “any.”

---

**NOTE:** You can create custom zones for some security devices. The list of zones from which you can select source and destination zones includes the predefined and custom zones that have been configured for all devices managed by NetScreen-Security Manager. Therefore, you should only select zones that are applicable for the device on which you will install the Security Policy.
Configuring Source & Destination Address Objects for IDP Rules

In the NetScreen-Security Manager system, address objects are used to represent components on your network: hosts, networks, servers, etc. Typically, a server or other device on your network is the destination IP for incoming attacks, and can sometimes be the source IP for interactive attacks (see “Configuring Backdoor Rules” on page 367 for more information on interactive attacks). You can specify “any” to monitor network traffic originating from any IP address. You can also “negate” the address object(s) listed in the Source or Destination column to specify all sources or destinations except the excluded object(s).

You can create address objects either before you create an IDP rule or while creating or editing an IDP rule. To select or configure an address object, right-click either the Source or Destination column of a rule and select Select Address. In the Select Source Addresses dialog box, you can either select an already-created address object or click the Add icon to create a new host, network, or group object.

**EXAMPLE: SETTING SOURCE AND DESTINATION**

You want to detect incoming attacks that target your internal network. Set the From Zone to Untrust and the Source IP to any. Set the To Zone to dmz and trust. Select the address object that represents the host or server you want to protect from attacks as the Destination IP. Your rule looks similar to this example:

Figure 76: Set Source and Destination

<table>
<thead>
<tr>
<th>No.</th>
<th>From Zone</th>
<th>Source</th>
<th>To Zone</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>untrust</td>
<td>any</td>
<td>dmz</td>
<td>Internal Network</td>
</tr>
</tbody>
</table>

**EXAMPLE: SETTING MULTIPLE SOURCES AND DESTINATIONS**

You want to detect attacks between two networks. Select multiple address objects for the Source and Destination. Your rule looks similar to this example:

Figure 77: Set Multiple Source and Destination Networks

<table>
<thead>
<tr>
<th>No.</th>
<th>From Zone</th>
<th>Source</th>
<th>To Zone</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>untrust</td>
<td>Europe Users</td>
<td>dmz</td>
<td>Internal Network</td>
</tr>
<tr>
<td></td>
<td>Europe Email Server</td>
<td>trust</td>
<td>Administrator</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Europe Workstation</td>
<td>Administrator</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The more specific you are in defining the source and destination of an attack, the more you reduce false positives.
Configuring Services for IDP Rules

Services are application layer protocols that define how data is structured as it travels across the network. Because the services you support on your network are the same services that attackers must use to attack your network, you can specify which services are supported by the destination IP to make your rule more efficient.

NOTE: All services rely on a transport layer protocol to transmit data. IDP includes services that use TCP, UDP, RPC, and ICMP transport layer protocols.

Service objects represent the services running on your network. NetScreen-Security Manager includes predefined service objects that are based on industry-standard services. You use these service objects in rules to specify the service an attack uses to access your network. You can also create custom service objects to represent protocols that are not included in the predefined services. For more information about configuring service objects, see “Configuring Service Objects” on page 281.

In the Service column you select the service of the traffic you want IDP to match:

- Select Default to accept the service specified by the attack object you select in the Attacks column. When you select an attack object in the Attack column, the service associated with that attack object becomes the default service for the rule. To see the exact service, view the attack object details.

- Select Any to set any service.

- Select Service to choose specific services from the list of defined service objects.

EXAMPLE: SETTING DEFAULT SERVICES
You want to protect your FTP server from FTP attacks. Set the service to Default, and add an attack object that detects FTP buffer overflow attempts. The Service column in the rule still displays “Default”, but the rule actually uses the default service of TCP-FTP, which is specified in the attack object. Your rule looks similar to this example:

Figure 78: Set Default Services

<table>
<thead>
<tr>
<th>From Zone</th>
<th>Source</th>
<th>To Zone</th>
<th>Destination</th>
<th>Service</th>
<th>Terminate Ma...</th>
<th>Action</th>
<th>Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>urtrust</td>
<td>any</td>
<td>dmz</td>
<td>trust</td>
<td>FTP Server</td>
<td>Default</td>
<td></td>
<td>None</td>
</tr>
</tbody>
</table>

| NOTE: All services rely on a transport layer protocol to transmit data. IDP includes services that use TCP, UDP, RPC, and ICMP transport layer protocols.

EXAMPLE: SETTING CUSTOM SERVICES
Your mail server supports POP3 and SMTP connections but not IMAP. Set POP3 and SMTP service objects as services that can be used to attack that server. Because IMAP is not supported, you do not need to add the IMAP service object.

Your rule looks similar to the example below:
If you are supporting services on non-standard ports, you should choose a service other than default.

EXAMPLE: SETTING NON-STANDARD SERVICES
You use a non-standard port (8080) for your HTTP services. Use the Object Manager to create a custom service object on port 8080.

Add this service object to your rule, then add several HTTP attack objects, which have a default service of TCP/80. IDP uses the specified service, HTTP-8080, instead of the default, and looks for matches to the HTTP attacks in TCP traffic on port 8080.
Your rule looks similar to this example:

<table>
<thead>
<tr>
<th>From Zone</th>
<th>Source</th>
<th>To Zone</th>
<th>Destination</th>
<th>Service</th>
<th>Terminate Match</th>
<th>Action</th>
<th>Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>untrust</td>
<td>any</td>
<td>dmz</td>
<td>Web Server</td>
<td>HTTP-8080</td>
<td></td>
<td>checked</td>
<td>None</td>
</tr>
</tbody>
</table>

Figure 81: Set Non-Standard Service
You can create your own service objects to use in rules, such as service objects for protocols that use non-standard ports. However, you cannot match attack objects to protocols they do not use.

Configuring Terminal IDP Rules
The normal IDP rule-matching algorithm starts from the top of the rulebase and checks traffic against all rules in the rulebase that match the source, destination, and service. A terminal rule is an exception to this normal rule-matching algorithm. When a match is discovered in a terminal rule for the source, destination, and service, IDP does not continue to check subsequent rules for the same source, destination, and service. It does not matter whether or not the traffic matches the attack objects in the matching rule.

You can use a terminal rule for the following purposes:

- To set different actions for different attacks for the same Source and Destination. This is illustrated by rules 3 and 6 in the “Setting Terminal Rules” example below.

- To disregard traffic that originates from a known trusted Source. Typically the action is None for this type of terminal rule. This is illustrated by rule 1 in the “Setting Terminal Rules” example below.

- To disregard traffic that is sent to a server that is only vulnerable to a specific set of attacks. Typically, the action is Drop Connection for this type of terminal rule.

Use caution when defining terminal rules. You can inadvertently leave your network open to attacks by creating an inappropriate terminal rule. Remember that traffic matching the source, destination, and service of a terminal rule is not compared to subsequent rules, even if the traffic does not match an attack object in the terminal rule. Use a terminal rule only when you want to examine a certain type of traffic for one specific set of attack objects and no others. Be particularly careful about terminal rules using “any” for both the source and destination.
Terminal rules should appear near the top of the rulebase, before other rules that would match the same traffic. You set a rule as terminal by selecting the box in the Terminate Match column of the Security Policy window when the rule is created or modified.

NOTE: In many cases, you can use an exempt rule instead of a terminal rule. You might find it easier and more straightforward to configure an exempt rule than a terminal rule. See “Configuring Exempt Rules” on page 364.

EXAMPLE: SETTING TERMINAL RULES
In the example IDP rulebase shown below, rules 1, 3, 4, and 5 are configured as terminal rules:

- Rule 1 terminates the match algorithm if the source IP of the traffic originates from the Security Network, a known trusted network. If this rule is matched, IDP disregards traffic from the Security Network and does not continue monitoring the session for malicious data.

- Rules 3 and 6 set different actions for different attacks when the destination IP is the Corporate or Europe E-mail server. Rule 3 terminates the match algorithm when the attack is an email that uses the SMTP context Confidential. Rule 6 closes the server when the attack is an SMTP attack.

- Rule 4 terminates the match algorithm when the destination is the Web Server and the attack is a Critical or High HTTP attack. The rule ensures that IDP drops the most important HTTP attacks against the Web Server and does not continue to match the connection.

- Rule 5 terminates the match algorithm when the source is the Internal Network and the attack is a Critical, High, or Medium Trojan Backdoor. The rule ensures that IDP closes both the client and server and does not continue to match the connection.

Figure 82: Set Terminal Rules
Defining Actions For IDP Rules

You can tell the security device which actions to perform against attacks that match rules in your Security Policy. For each attack that matches a rule, you can choose to ignore, drop, or close the current attacking packets or connection. If the rule is triggered, the device can perform actions against the connection.

Remember that the device can drop traffic only when IDP is enabled in inline mode; when IDP is enabled in inline tap (sniffer) mode, it cannot perform drop or close actions.

You can specify the following actions for IDP rules:

Table 28: IDP Rule Actions

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>IDP takes no action against the connection. If a rule that contains an action of None is matched, the corresponding log record displays “accept” in the action column of the Log Viewer.</td>
</tr>
<tr>
<td>Ignore</td>
<td>IDP ignores the remainder of a connection after an attack object in an IDP rule is matched. Use with caution.</td>
</tr>
<tr>
<td>Drop Packet</td>
<td>IDP drops a matching packet before it can reach its destination but does not close the connection. Use this action to drop packets for attacks in traffic that is prone to spoofing, such as UDP traffic. Dropping a connection for such traffic could result in a denial of service that prevents you from receiving traffic from a legitimate source IP address.</td>
</tr>
<tr>
<td>Drop Connection</td>
<td>IDP drops the connection without sending a RST packet to the sender, preventing the traffic from reaching its destination. Use this action to drop connections for traffic that is not prone to spoofing.</td>
</tr>
<tr>
<td>Close Client</td>
<td>IDP closes the connection to the client, but not to the server.</td>
</tr>
<tr>
<td>Close Server</td>
<td>IDP closes the connection to the server, but not to the client.</td>
</tr>
<tr>
<td>Close Client and Server</td>
<td>IDP closes the connection and sends a RST packet to both the client and the server. If IDP is operating in inline tap mode, IDP sends a RST packet to both the client and server but does NOT close the connection.</td>
</tr>
<tr>
<td>Diffserv Marking</td>
<td>Assigns the service differentiation value indicated to the packet, then passes it on normally. The value is set in the dialog that appear when you select this action in the rulebase.</td>
</tr>
<tr>
<td>Recommended</td>
<td>IDP takes the action recommended by Juniper Networks. With IDP 4.1, attack objects have a recommended action associated with them. If a packet triggers more than one attack object, IDP applies the most secure of the recommended actions. Available with IDP 4.1 and later. This setting has no meaning for IDP 4.0 or earlier. Rules with this setting will not be loaded onto devices running earlier versions of IDP.</td>
</tr>
</tbody>
</table>

Configuring Attack Objects in IDP Rules

Attack objects represent specific patterns of malicious activity within a connection, and are a method for detecting attacks. Each attack object detects a known or unknown attack that can be used to compromise your network. For more information about attack objects, see “Working with IDP Attack Objects” on page 237.
To add attack objects to a rule, right-click the Attacks column of the rule and select Select Attacks. In the Add Attacks dialog box, you can add attacks using one or both of the following options:

- **Attack List**—Select this option to add individual attack objects from an alphabetically list of all predefined and custom attack objects. Attack objects are listed alphabetically by name of attack.

  Selecting individual attacks is a good option if you know the exact name of the attack you want to add to a rule. To locate a specific word or string in the attack object name, use the integrated search function in NetScreen-Security Manager; for details, see “Searching in the User Interface” on page 25.

- **Attack Groups**—Select this option to add attack object groups from three predefined dynamic attack groups (Category, OS, Severity); if you have created a custom dynamic group, that group is also listed.

  Selecting attack groups is a good option when you are unsure of the exact attack you want to add to a rule, but you know the type of attack protection you want the security device to provide. Within the Attack Groups, you can:

  - Add all Attack Objects (select All Attacks). Consider carefully before select this option; using all attack objects in a rule can severely impact performance on the security device.
  - Add one or more attack groups (hold down CTL to select multiple groups). Predefined dynamic groups might contain subgroups as well.
  - Add individual attack objects (hold down CTL to select multiple objects)

The following sections detail each predefined dynamic attack group.

### Adding IDP Attack Object Groups by Category

The Category group includes attack objects organized by services. Services are application layer protocols that define how data is structured as it travels across the network. A protocol is a specification that indicates how communication between two entities (applications, servers, Ethernet cards, etc.) occurs.

When attacking a system, attackers use the protocol of a supported service to communicate their malicious activity to the server. However, attackers can only use protocols that are supported by the system they are attacking. You can add a category group to the Attacks column in your rule; however, you need to select only the categories that are used by the address objects you are protecting with the rule.

For example, if you rely extensively on FTP and HTTP for file transfers to and from your Web servers, choose the FTP and HTTP category groups to carefully monitor all traffic that uses these services.

### Adding IDP Attack Objects by Operating System

The Operating System group includes attack objects for several predefined operating systems to help you choose the attack objects that are the most dangerous to specific components on your network. You can choose BSD, Linux, Solaris, or Windows.
Adding IDP Attack Objects by Severity

The Severity group includes five attack object groups organized by severity level. You can select one or more groups to include in your rule. To protect critical address objects or “popular” attacker targets, such as your mail server, use multiple severity levels to ensure maximum protection.

We recommend using the following actions and notification settings when using severity-based dynamic attack groups in a rule:

Table 29: Severity Levels, Recommended Actions and Notifications

<table>
<thead>
<tr>
<th>Severity</th>
<th>Description</th>
<th>Rec. Action</th>
<th>Rec. Notification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>Attacks attempt to evade an IDS, crash a machine, or gain system-level privileges.</td>
<td>Drop Packet</td>
<td>Logging Alert</td>
</tr>
<tr>
<td>Major</td>
<td>Attacks attempt to crash a service, perform a denial-of-service, install or use a Trojan, or gain user-level access to a host.</td>
<td>Drop Packet, Drop Connection</td>
<td>Logging Alert</td>
</tr>
<tr>
<td>Minor</td>
<td>Attacks attempt to obtain critical information through directory traversal or information leaks.</td>
<td>(no recommended action)</td>
<td>Logging</td>
</tr>
<tr>
<td>Warning</td>
<td>Attacks attempt to obtain non-critical information or scan the network with a scanning tool. They can also be obsolete attacks or anomalous (but probably harmless) traffic.</td>
<td>(no recommended action)</td>
<td>Logging</td>
</tr>
<tr>
<td>Info</td>
<td>Attacks are normal, harmless traffic containing URLs, DNS lookup failures, and SNMP public community strings. You can use informational attack objects to obtain information about your network.</td>
<td>(no recommended action)</td>
<td>(no recommended notification)</td>
</tr>
</tbody>
</table>

You configure actions in the Action column of the rule; see “Defining Actions For IDP Rules” on page 356. You configure notification settings in the Notification column of the rule; see “Configuring Notification in IDP Rules” on page 360.

Adding Custom Dynamic Attack Groups

You can add previously-created custom dynamic attack groups to a rule.

Additionally, after you have added the custom group to a rule, you can edit the settings for the dynamic group by double-clicking the group icon in the rule.

Configuring IP Actions in IDP Rules

(This column only appears when you view the Security Policy in Expanded Mode. To change the Security Policy view from Compact Mode to Expanded Mode, from the menu bar, select View > Expanded Mode.)

If the current network traffic matches a rule, the security device can perform an IP action against future network traffic that uses the same IP address. IP actions are similar to other actions; they direct the device to drop or close the connection. However, because you now also have the attacker’s IP address, you can choose to block the attacker for a specified amount of time. If attackers cannot immediately regain a connection to your network, they might try to attack easier targets.
Use IP actions in conjunction with actions and logging to secure your network. In a rule, first configure an action to detect and prevent current malicious connections from reaching your address objects. Then, right-click in the IP Action column of the rule and select Configure to bring up the Configure IP Action dialog box. Enable and configure an IP action to prevent future malicious connections from the attacker’s IP address.

Choosing an IP Action
For each IP action option, an IP action is generated by the NetScreen-Security Manager system. The IP action instructs the security device to perform the specified task. Select from the following options:

- **IDP Notify**—The security device does not take any action against future traffic, but logs the event. This is the default.

- **IDP Drop**—The security device drops the matching connection and blocks future connections that match the criteria set in the Block list.

- **IDP Close**—The security device closes future connections that match the criteria in the Block list.

Choosing a Block Option
Each block option follows the criteria you set in the Actions box. Block options can be based on the following matches of the attack traffic:

- **Source, Destination, Destination Port and Protocol**—The security device blocks future traffic based on the source, destination, destination port, and protocol of the attack traffic. This is the default.

- **Source**—The security device blocks future traffic based on the source of the attack traffic.

- **Destination**—The security device blocks future traffic based on the destination of the attack traffic.

- **From Zone, Destination, Destination Port and Protocol**—The security device blocks future traffic based on the source zone, destination, destination port, and protocol of the attack traffic.

- **From Zone**—The security device blocks future traffic based on the source zone of the attack traffic.

Setting Logging Options
When the security device detects attack traffic that matches a rule and an IP action is triggered, the device can log information about the IP action that was taken or create an alert in the Log Viewer. By default, there are no logging options set.

Setting Timeout Options
You can set the number of seconds that you want the IP action to remain in effect after a traffic match. For permanent IP actions, leave the timeout at 0 (this is the default).
Configuring Notification in IDP Rules

You can choose to log an attack and create log records with attack information that you can view real-time in the Log Viewer. For more critical attacks, you can also set an alert flag to appear in the log record.

To log an attack for a rule, right-click the Notification column of the rule and select Configure. The Configure Notification dialog box appears.

The first time you design a Security Policy, you might be tempted to log all attacks and let the policy run indefinitely. Don’t do this! Some attack objects are informational only, and others can generate false positives and redundant logs. If you become overloaded with data, you can miss something important. Remember that Security Policies that generate too many log records are hazardous to the security of your network, as you might discover an attack too late or miss a security breach entirely due to sifting through hundreds of log records. Excessive logging can also affect throughput, performance, and available disk space. A good Security Policy generates enough logs to fully document only the important security events on your network.

- **Setting Logging**—In the Configure Notification dialog box, select Logging and then click OK. Each time the rule is matched, the NetScreen-Security Manager system creates a log record that appears in the Log Viewer.

- **Setting an Alert**—In the Configure Notification dialog box, select Alert and then click OK. If Alert is selected and the rule is matched, the security device places an alert flag in the Alert column of the Log Viewer for the matching log record.

- **Logging Packets**—You can record the individual packets in the network traffic that matched a rule by capturing the packet data for the attack. Viewing the packets used in an attack on your network can help you determine the extent of the attempted attack and its purpose, whether or not the attack was successful, and any possible damage to your network.

  **NOTE:** To improve performance, log only the packets after the attack.

  If multiple rules with packet capture enabled match the same attack, the security device captures the maximum specified number of packets. For example, you configure Rule 1 to capture 10 packets before and after the attack, and Rule 2 to capture 5 packets before and after the attack. If both rules match the same attack, IDP attempts to capture 10 packets before and after the attack.

  **NOTE:** Packet captures are restricted to 256 packets before and after the attack.

Setting VLAN Tags for IDP Rules

You can choose to apply rules to traffic on certain VLANs only. Normally, for a rule to take effect, it must match the packet source, destination, service, and attack objects. If the VLAN cell is populated with a value other than any, then the rule will also consider the packet’s VLAN tag when determining a match.
The IDP, Exempt, Backdoor, SYN Protector, Traffic Anomalies, and Network Honeypot rulesbases support VLAN matching. VLAN matching is only supported in Transparent and Sniffer modes.

**NOTE:** VLAN matching is supported in IDP 4.1 and later. Rules with a VLAN Tag field set to anything other than any are removed from the rulebase before NSM sends the security policy to an IDP device that does not support VLAN tags.

VLAN tag matching can be set to any, none, a particular VLAN tag value, or a range of VLAN tag values. Use VLAN objects to create individual VLAN tags or ranges of VLAN tags. You can assign more than one VLAN object to a rule. To assign a VLAN object to a rule, or to set the VLAN Tag value to none, right-click in the VLAN Tag cell of the rule.

Figure 83: VLAN Tags in a Rule

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Terminate</th>
<th>Action</th>
<th>Notification</th>
<th>VLAN Tag</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>any</td>
<td>any</td>
<td></td>
<td></td>
<td>None</td>
<td>1</td>
<td>any</td>
</tr>
</tbody>
</table>

VLAN matching works as follows:

- **Any:** Matches traffic with any or no VLAN tag (default)
- **Single tag:** Matches traffic with that specific tag only
- **Range of tags:** Matches traffic with any tag in that range
- **None:** Matches only traffic that has no VLAN tag.

See Configuring VLAN Objects on page 302 to create VLAN objects for use in security policies.

**Setting Severity for IDP Rules**

(This column only appears when you view the Security Policy in Expanded Mode. To change the Security Policy view from Compact Mode to Expanded Mode, from the menu bar, select View > Expanded Mode.)

You can override the inherent attack severity on a per-rule basis within the IDP rulebase. You can set the severity to either Default, Info, Warning, Minor, Major, or Critical.

To change the severity for a rule, right-click the Severity column of the rule and select a severity.
**Setting Target Security Devices for IDP Rules**

For each rule in the IDP rulebase, you can select the security device on which the rule is installed. When you install the Security Policy that the rule belongs to, the rule becomes active only on the device(s) you selected in the Install On column of the rulebase.

---

**NOTE:** The NetScreen-Security Manager supports IDP only on ISG family security devices running ScreenOS 5.0.0-IDP1 and on standalone IDP Sensors running IDP 4.0 or higher.

---

**Entering Comments for IDP Rules**

You can enter notations about the rule in the Comments column. Anything you enter in the Comments column is not pushed to the target device(s). To enter a comment, right-click the Comments column and select Edit Comments. The Edit Comments dialog box appears. You can enter up to 1024 characters in the Comments field.

**EXAMPLE: CONFIGURING RULES FOR AN ISG IN STANDALONE IDP MODE**

You can deploy the ISG 2000 or ISG 1000 security device as a standalone IDP security system protecting critical segments of your private network. For example, you might already have a security device actively screening traffic between the Internet and your private network (some device can optionally use Deep Inspection to inspect this traffic), but you still need to protect internal systems, such as mail servers, from attacks that might originate from user machines in an otherwise trusted network. In this case, you need a security system that provides IDP instead of firewall functions.

Standalone IDP Sensors function in this mode by default and do not have to be specifically configured for it.

In this example, you are deploying a ISG 2000 device as a standalone IDP security system between the Trust zone and the custom “Data_Center” zone in your network. Your company’s file, mail, and database servers reside in the Data_Center zone. While you want to allow users in the Trust zone to be able to access the servers in the Data_Center zone, you also need to protect the servers from attacks that inadvertently might have been introduced into a user machine in the Trust zone. You create a firewall rule from the Trust to the Data_Center zone that allows traffic from any source to any destination for any service, then enable IDP in the Rule Options column, as shown in the following:

*Figure 84: Firewall Rule for Dedicated IDP*

<table>
<thead>
<tr>
<th>No.</th>
<th>Match</th>
<th>Action</th>
<th>Install On</th>
<th>Rule Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>trust any Data_Center any any</td>
<td>permit</td>
<td>ISG-2000</td>
<td>(IDP Ena...</td>
</tr>
</tbody>
</table>

You would then add and configure IDP rulebases for the Security Policy to detect possible attacks against servers in the Data_Center zone.

*Figure 85: IDP Rules for Dedicated IDP*
### Chapter 9: Configuring Security Policies

#### Configuring IDP Rules

<table>
<thead>
<tr>
<th>Match</th>
<th>Action</th>
<th>Attacks</th>
<th>Notification</th>
</tr>
</thead>
<tbody>
<tr>
<td>From Zone: any</td>
<td>Close Session</td>
<td>TROJAN</td>
<td>Logging</td>
</tr>
<tr>
<td>Source: any</td>
<td></td>
<td>VIRUS - ...</td>
<td>Alert</td>
</tr>
<tr>
<td>To Zone: any</td>
<td></td>
<td>WORM - ...</td>
<td></td>
</tr>
<tr>
<td>Destination: any</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service: Default</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Terminate Matches:</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

*Configuring IDP Rules*  
Page 363
Configuring Exempt Rules

The Exempt rulebase works in conjunction with the IDP rulebase. Before you can create exempt rules, you must first create rules in the IDP rulebase. If traffic matches a rule in the IDP rulebase, IDP attempts to match the traffic against the Exempt rulebase before performing the specified action or creating a log record for the event.

NOTE: If you delete the IDP rulebase, the Exempt rulebase is also deleted.

You might want to use an exempt rule when an IDP rule uses an attack object group that contains one or more attack objects that produce false positives or irrelevant log records. To prevent unnecessary alarms, you might want to use an exempt rule to exclude a specific source, destination, or source/destination pair from matching an IDP rule.

When you create an exempt rule, you must specify the following:

- Source and destination for traffic you want to exempt. You can set the source or destination to “any” to exempt network traffic originating from any source or sent to any destination. You can also specify “negate” to specify all sources or destinations except the specified addresses.

- The attacks you want IDP to exempt for the specified source/destination addresses. You must include at least one attack object in an exempt rule.

NOTE: The Exempt rulebase is a non-terminal rulebase. That is, IDP attempts to match traffic against all rules in the Exempt rulebase and all matches are executed.

Adding the Exempt Rulebase

Before you can configure a rule in the Exempt rulebase, you need to add the Exempt rulebase to a Security Policy.

1. In the main navigation tree, select Security Policies. Open a security policy by double-clicking the policy name in the Security Policies window or click the policy name and then select the Edit icon.

2. Click the Add icon in the upper right corner of the Security Policy window and select Add Exempt Rulebase to enable the Exempt rulebase tab.

3. To configure an exempt rule, click the Add icon on the left side of the Security Policy window to open a default exempt rule. You can modify this rule as necessary.

Defining Match

You specify the traffic you want to exempt from attack detection. The Match columns From Zone, Source, To Zone, and Destination are required for all rules in the exempt rulebase.

The following sections detail the Match columns of an exempt rule.
Configuring Source & Destination Zones

You can select multiple zones for the source and destination, however these zones must be available on the security devices on which you will install the policy. You can specify “any” for the source or destination zones to monitor network traffic originating or destined for any zone.

NOTE: You can create custom zones for some security devices. The list of zones from which you can select source and destination zones includes the predefined and custom zones that have been configured for all devices managed by NetScreen-Security Manager. Therefore, you should only select zones that are applicable for the device on which you will install the Security Policy.

Configuring Source & Destination Address Objects

In the NetScreen-Security Manager system, address objects are used to represent components on your network: hosts, networks, servers, etc. You can specify “any” to monitor network traffic originating from any IP address. You can also negate the address object(s) listed in the Source or Destination column to specify all sources or destinations except the excluded object.

You can create address objects either before you create an exempt rule or while creating or editing an exempt rule. To select or configure an address object, right-click either the Source or Destination column of a rule and select Select Address. In the Select Source Addresses dialog box, you can either select an already-created address object or click the Add icon to create a new host, network, or group object.

EXAMPLE: EXEMPTING A SOURCE/DESTINATION PAIR

To improve performance and eliminate false positives between your Internal Lab devices and your Engineering desktops, you want to exempt attack detection. Your exempt rule looks similar to the one below:

Figure 86: Exempting Source and Destination

Setting Attack Objects

You specify the attack(s) you want IDP to exempt for the specified source/destination addresses. You must include at least one attack object in an exempt rule.
Example: Exempting Specific Attack Objects
You consistently find that your Security Policy generates false positives for the attack HTTP Buffer Overflow: Header on your internal network. You want to exempt attack detection for this attack when the source IP is from your internal network. Your exempt rule looks similar to the one below:

Figure 87: Exempting Attack Object

Specifying VLANs
You can specify that the rule be applied only to packets from particular VLANs. See Setting VLAN Tags for IDP Rules on page 361 for more information.

Setting Target Devices
For each rule in the rulebase, you can select the IDP-capable device that will use that rule to detect and prevent attacks. Alternatively, you can use Device Manager to assign policies to devices.

Entering Comments
You can enter notations about the rule in the Comments column. Anything you enter in the Comments column is not pushed to the target device(s). To enter a comment, right-click the Comments column and select Edit Comments. The Edit Comments dialog box appears. You can enter up to 1024 characters in the Comments field.

Creating an Exempt Rule from the Log Viewer
You can also create a rule in the Exempt rulebase directly from the NetScreen-Security Manager Log Viewer. You might want to use this method to quickly eliminate rules that generate false positive log records. (For more information about viewing IDP logs, see “Review IDP Logs” on page 44.) For more information about using the Log Viewer, see “Logging” on page 587.

To create an exempt rule from the Log Viewer:
1. View the IDP/DI logs in the Log Viewer.
2. Right-click a log record that contains an attack you want to exempt and select Exempt.
Configuring Backdoor Rules

A backdoor is a mechanism installed on a host computer that facilitates unauthorized access to the system. Attackers who have already compromised a system can install a backdoor to make future attacks easier. When attackers type commands to control a backdoor, they generate interactive traffic.

Interactive traffic is traffic that indicates human involvement in a normally automated process, such as a user typing commands. Interactive traffic looks different than other traffic because humans are manually controlling one end of the connection. In a connection between two programs, the data transfer is automated; TCP packets can be batched and sent in bulk for efficiency. In a connection between a program and a user, packets are sent when they become available; characters display as they are typed (not after the word is complete). Interactive programs transmit several short IP packets containing individual keystrokes and their echoes, reflecting the real-time actions of a user (or attacker).
When attackers type commands to control a backdoor, they generate interactive traffic that IDP can detect. Unlike anti-virus software, which scans for known backdoor files or executables on the host system, IDP detects the interactive traffic that is produced when backdoors are used. This method ensures that IDP can detect all backdoors, both known and unknown. If interactive traffic is detected, IDP can perform IDP actions against the connection to prevent the attacker from further compromising your network.

When you configure a backdoor rule, you must specify the following:

- Source and destination addresses for traffic you want to monitor. To detect incoming interactive traffic, set the Source to “any” and the Destination to the IP address of network device you want to protect. To detect outgoing interactive traffic, set the Source to the IP address of the network device you want to protect and the Destination to “any”.

- Services that are offered by the Source or Destination as well as interactive services that can be installed and used by attackers.

NOTE: Do not include TELNET, SSH, RSH, NETMEETING, or VNC as services, as these services are often used to legitimately control a remote system. Including these services can generate false positives.

NOTE: The Backdoor rulebase is a terminal rulebase. That is, when IDP finds a match on a rule in the Backdoor rulebase, it does not execute succeeding rules.

Adding the Backdoor Rulebase

Before you can configure a rule in the Backdoor rulebase, you need to add the Backdoor rulebase to a Security Policy.

1. In the main navigation tree, select Security Policies. Open a security policy by double-clicking the policy name in the Security Policies window or click the policy name and then select the Edit icon.

2. Click the Add icon in the upper right corner of the Security Policy window and select Add Backdoor Rulebase. The Backdoor rulebase tab appears.

3. To configure a backdoor rule, click the Add icon on the left side of the Security Policy window. A default backdoor rule appears. You can modify this rule as needed.

Defining Match

You specify the traffic you want to IDP to monitor for indications of backdoors or Trojans. The Match columns From Zone, Source, To Zone, Destination, and Service are required for all rules in the Backdoor rulebase.
The following sections detail the Match columns of a backdoor rule.

### Configuring Source & Destination Zones

You can select multiple zones for the source and destination, however these zones must be available on the security devices on which you will install the policy. You can specify “any” for the source or destination zones to monitor network traffic originating or destined for any zone.

**NOTE:** You can create custom zones for some security devices. The list of zones from which you can select source and destination zones includes the predefined and custom zones that have been configured for all devices managed by NetScreen-Security Manager. Therefore, you should only select zones that are applicable for the device on which you will install the Security Policy.

### Configuring Source & Destination Address Objects

In the NetScreen-Security Manager system, address objects are used to represent components on your network: hosts, networks, servers, etc. Typically, a server or other device on your network is the destination IP for incoming attacks, and can sometimes be the source IP for interactive attacks. You can specify “any” to monitor network traffic originating from any IP address. You can also negate the address object(s) listed in the Source or Destination column to specify all sources or destinations except the excluded address object.

You can create address objects either before you create a backdoor rule or while creating or editing a backdoor rule. To select or configure an address object, right-click either the Source or Destination column of a rule and select Select Address. In the Select Source Addresses dialog box, you can either select an already-created address object or click the Add icon to create a new host, network, or group object.

### Configuring Services

Select interactive service objects. Be sure to include services that are offered by the source or destination IP as well as interactive services that are not; attackers can use a backdoor to install any interactive service. Do not include telnet, SSH, RSH, netmeeting, or VNC, as these services are often used to remotely control a system legitimately and their inclusion might generate false positives.

### Setting Operation

Set the Operation to detect or ignore. If you select detect, choose an action to perform if backdoor traffic is detected. If you are protecting a large number of address objects from interactive traffic, you can create a rule that ignores accepted forms of interactive traffic from those objects, then create a succeeding rule that detects all interactive traffic from those objects.
Setting Actions

Choose an action to perform if IDP detects interactive traffic:

Table 30: Actions for Backdoor Rule:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept</td>
<td>IDP accepts the interactive traffic.</td>
</tr>
<tr>
<td>Drop Connection</td>
<td>IDP drops the interactive connection without sending a RST packet to the</td>
</tr>
<tr>
<td></td>
<td>sender, preventing the traffic from reaching its destination. Use this action</td>
</tr>
<tr>
<td></td>
<td>to drop connections for traffic that is not prone to spoofing.</td>
</tr>
<tr>
<td>Close Client and</td>
<td>IDP closes the interactive connection and sends a RST packet to both the</td>
</tr>
<tr>
<td>Server</td>
<td>client and the server. If the IDP is in sniffer mode, IDP sends a RST packet</td>
</tr>
<tr>
<td></td>
<td>to both the client and server but does NOT close the connection.</td>
</tr>
<tr>
<td>Close Client</td>
<td>IDP closes the interactive connection to the client, but not to the server.</td>
</tr>
<tr>
<td>Close Server</td>
<td>IDP closes the interactive connection to the server, but not to the client.</td>
</tr>
</tbody>
</table>

Setting Notification

You can choose to log an attack and create log records with attack information that you can view real-time in the Log Viewer. For more critical attacks, you can also set an alert flag to appear in the log record.

To log an attack for a rule, right-click the Notification column of the rule and select Configure. The Configure Notification dialog box appears.

The first time you design a Security Policy, you might be tempted to log all attacks and let the policy run indefinitely. Don’t do this! Some attack objects are informational only, and others can generate false positives and redundant logs. If you become overloaded with data, you can miss something important. Remember that Security Policies that generate too many log records are hazardous to the security of your network, as you might discover an attack too late or miss a security breach entirely due to sifting through hundreds of log records. Excessive logging can also affect IDP throughput, performance, and available disk space. A good Security Policy generates enough logs to fully document only the important security events on your network.

Setting Logging

In the Configure Notification dialog box, select Logging and then click OK. Each time the rule is matched, the IDP system creates a log record that appears in the Log Viewer.

You can choose to log an attack and create log records with attack information that you can view real-time in the Log Viewer. For more critical attacks, however, you might want to be notified immediately by email, have IDP run a script in response to the attack, or set an alarm flag to appear in the log record. Your goal is to fine-tune the attack notifications in your Security Policy to your individual security needs.

Setting an Alert

In the Configure Notification dialog box, select Alert and then click OK. If Alert is selected and the rule is matched, IDP places an alert flag in the alert column of the Log Viewer for the matching log record.
Chapter 9: Configuring Security Policies

Logging Packets
You can record the individual packets in the network traffic that matched a rule by capturing the packet data for the attack. Viewing the packets used in an attack on your network can help you determine the extent of the attempted attack and its purpose, whether or not the attack was successful, and any possible damage to your network.

NOTE: To improve IDP performance, log only the packets after the attack.

If multiple rules with packet capture enabled match the same attack, IDP captures the maximum specified number of packets. For example, you configure Rule 1 to capture 10 packets before and after the attack, and Rule 2 to capture 5 packets before and after the attack. If both rules match the same attack, IDP attempts to capture 10 packets before and after the attack.

NOTE: Packet captures are restricted to 256 packets before and after the attack.

Setting Severity
You can override the inherent attack severity on a per-rule basis within the Backdoor rulebase. You can set the severity to either Default, Info, Warning, Minor, Major, or Critical.

To change the severity for a rule, right-click the Severity column of the rule and select a severity.

Specifying VLANs
You can specify that the rule be applied only to packets from particular VLANs. See Setting VLAN Tags for IDP Rules on page 361 for more information.

Setting Target Devices
For each rule in the rulebase, you can select the IDP-capable device that will use that rule to detect and prevent attacks. Alternatively, you can use Device Manager to assign policies to devices.

Entering Comments
You can enter notations about the rule in the Comments column. Anything you enter in the Comments column is not pushed to the target device(s). To enter a comment, right-click the Comments column and select Edit Comments. The Edit Comments dialog box appears. You can enter up to 1024 characters in the Comments field.
Configuring SYN Protector Rules

The SYN-Protector rulebase protects your network from SYN floods by ensuring that the three-way handshake is performed successfully for specified TCP traffic. If you know that your network is vulnerable to a SYN flood, use the SYN Protector rulebase to prevent it.

**NOTE:** The SYN Protector Rulebase is a terminal rulebase; when IDP finds a match on a rule, it does not execute succeeding rules.

The TCP Handshake

When a TCP connection is initiated, a three-way handshake takes place:

- A client host sends a SYN packet to a specific port on the server to request a connection.

- Next, the server sends the client host a SYN/ACK packet, which both acknowledges (ACK) the original SYN packet from the client host and forwards a new SYN packet. The potential connection is now in a SYN_RECV state.

- Finally, the client host sends an ACK packet to the server to acknowledge receipt of the SYN/ACK packet. The connection is now in an ESTABLISHED state.

This three-way handshake contains an inherent, exploitable vulnerability that attackers can use to disable the system: a SYN flood. Most systems allocate a large, but finite number of resources to a connection table that is used to manage potential connections. While the connection table can sustain hundreds of concurrent connections across multiple ports, attackers can generate enough connection requests to exhaust all allocated resources.

**SYN-Floods**

Attackers initiate a SYN flood by manipulating the basic three-way handshake:

- A client host sends a SYN packet to a specific port on the server. However, the attacker ensures that the client host’s IP address is a spoofed IP address of an unreachable system.

- Next, the server sends the client host (spoofed address) a SYN/ACK packet. The potential connection is now in a SYN_RECV state.

- Since the system is unreachable, the server never receives an ACK or RST packet back from the client host. The potential connection is now in the SYN_RECV state, and is placed into a connection queue while it waits for an ACK or RST packet. This potential connection remains in the queue until the connection-establishment timer expires (when it will be deleted).

- The attacker sends another SYN packet to the server, requesting another connection. And then another. And another. The connection table fills to capacity and cannot accept new SYN requests. The server is overwhelmed, and quickly becomes disabled.
By default, the SYN Protector rulebase is only activated when the number of SYN packets per second is greater than 1020. This number is the sum of two parameters that you can set in the Sensor Settings Run-Time Parameters:

- Lower SYN’s-per-second threshold below which SYN Protector will be deactivated (the default value is 1000)
- Upper SYN’s-per-second threshold above which SYN Protector will be activated (the default value is 20)

Once the SYN Protector rulebase is activated, it remains active until the number of SYN packets per second is less than the Lower SYN’s-per-second threshold (which is 1000 by default).

**Adding the SYN Protector Rulebase**

Before you can configure a rule in the SYN Protector rulebase, you need to add the SYN Protector rulebase to a Security Policy.

1. In the main navigation tree, select *Security Policies*. Open a security policy by double-clicking the policy name in the Security Policies window or click the policy name and then select the Edit icon.

2. Click the Add icon in the upper right corner of the *Security Policy* window and select *Add SYN Protector Rulebase* to open the *SYN Protector rulebase* tab.

3. To configure a SYN Protector rule, click the Add icon on the left side of the *Security Policy* window to open a default SYN Protector rule. You can modify this rule as needed.

Figure 89 shows a default SYN Protector rulebase that has been modified.

<table>
<thead>
<tr>
<th>No.</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Mode</th>
<th>Notification</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>any</td>
<td>Web Server ...</td>
<td>TCP-ANY</td>
<td>relay</td>
<td>Logging</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FTP Server</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Defining Match**

Specify the traffic you want IDP to monitor for SYN floods.

**Configuring Source & Destination Address Objects**

Set the Source object to Any. Set the Destination Object to any Address Objects you want to protect.
Configuring Services

The default service, TCP-any, looks for SYN floods in all TCP-based traffic.

### Setting Mode

Select the mode that indicates how IDP handles TCP traffic:

- **None.** IDP takes no action, and does not participate in the three-way handshake.

- **Relay.** IDP acts as the middleman, or relay, for the connection establishment, performing the three-way handshake with the client host on behalf of the server. Relay mode guarantees that the server allocates resources only to connections that are already in an ESTABLISHED state. The relay is transparent to both the client host and the server.

  IDP receives the initial SYN packet sent by the client host and returns a SYN/ACK packet. If the client host sends an ACK packet, IDP completes the three-way handshake and allows the connection to move to an ESTABLISHED state. If IDP does not receive an ACK packet from the client host, as would be the case during a SYN flood attack, IDP does not complete the three-way handshake and the connection is not established.

- **Passive.** IDP handles the transfer of packets between the client host and the server, but does not actively prevent the connection from being established. Instead, IDP uses a timer to ensure that connections are established promptly, minimizing the use of server resources. The timer IDP uses for the connection establishment is shorter than the timer the server uses for the connection queue.

  IDP transfers the SYN packet sent by the client host to the server, then transfers the SYN/ACK packet sent by the server to the client host. If the client host sends an ACK packet to the server before the IDP connection timer expires, the connection is established. If the client host does not send an ACK packet to the server, as would be the case during a SYN flood attack, the IDP connection timer expires. IDP resets the connection to free resources on the server.

### Setting Notification

You can choose to log an attack and create log records with attack information that you can view real-time in the Log Viewer. For more critical attacks, you can also set an alert flag to appear in the log record.

To log an attack for a rule, right-click the Notification column of the rule and select Configure. The Configure Notification dialog box appears.

---

**NOTE:** Always set the SYN Protector service value to TCP-any. Selecting individual services can cause unpredictable interactions with other rulebases.
The first time you design a Security Policy, you might be tempted to log all attacks and let the policy run indefinitely. Don’t do this! Some attack objects are informational only, and others can generate false positives and redundant logs. If you become overloaded with data, you can miss something important. Remember that Security Policies that generate too many log records are hazardous to the security of your network, as you might discover an attack too late or miss a security breach entirely due to sifting through hundreds of log records. Excessive logging can also affect IDP throughput, performance, and available disk space. A good Security Policy generates enough logs to fully document only the important security events on your network.

Setting Logging
In the Configure Notification dialog box, select Logging and then click OK. Each time the rule is matched, the IDP system creates a log record that appears in the Log Viewer.

You can choose to log an attack and create log records with attack information that you can view real-time in the Log Viewer. For more critical attacks, however, you might want to be notified immediately by email, have IDP run a script in response to the attack, or set an alarm flag to appear in the log record. Your goal is to fine-tune the attack notifications in your Security Policy to your individual security needs.

Setting an Alert
In the Configure Notification dialog box, select Alert and then click OK. If Alert is selected and the rule is matched, IDP places an alert flag in the alert column of the Log Viewer for the matching log record.

Logging Packets
You can record the individual packets in the network traffic that matched a rule by capturing the packet data for the attack. Viewing the packets used in an attack on your network can help you determine the extent of the attempted attack and its purpose, whether or not the attack was successful, and any possible damage to your network.

If multiple rules with packet capture enabled match the same attack, IDP captures the maximum specified number of packets. For example, you configure Rule 1 to capture 10 packets before and after the attack, and Rule 2 to capture 5 packets before and after the attack. If both rules match the same attack, IDP attempts to capture 10 packets before and after the attack.

Packet captures are restricted to 256 packets before and after the attack.
Setting Severity

You can override the inherent attack severity on a per-rule basis within the SYN Protector rulebase. You can set the severity to either Default, Info, Warning, Minor, Major, or Critical.

To change the severity for a rule, right-click the Severity column of the rule and select a severity.

Specifying VLANs

You can specify that the rule be applied only to packets from particular VLANs. See Setting VLAN Tags for IDP Rules on page 361 for more information.

Setting Target Devices

For each rule in the rulebase, you can select the IDP-capable device that will use that rule to detect and prevent attacks. Alternatively, you can use Device Manager to assign policies to devices.

Entering Comments

You can enter notations about the rule in the Comments column. Anything you enter in the Comments column is not pushed to the target device(s). To enter a comment, right-click the Comments column and select Edit Comments. The Edit Comments dialog box appears. You can enter up to 1024 characters in the Comments field.

Configuring Traffic Anomalies Rules

Traffic anomaly rules protect your network from attacks by using traffic flow analysis to identify attacks that occur over multiple connections and sessions (such as scans).

NOTE: The Traffic Anomalies Rulebase is a terminal rulebase; when IDP finds a match on a rule, it does not execute succeeding rules.

Before attempting to enter an unknown network, attackers often gather information about the network and analyze any weaknesses to help them choose the best attack method. A port scan or network scan is often the first reconnaissance performed. Attackers typically use a scanning tool that attempts to connect to every port on a single machine (port scanning) or connect to multiple IP addresses on a network (network scanning). By determining which services are allowed and responding on your network, attackers can gain valuable information about your network configuration.

To detect scans and other distributed network attacks, the Traffic Anomalies Rulebase looks for patterns that indicate abnormal network activity. Attackers often use scanning tools to automate their port scans, allowing them to scan multiple ports quickly and efficiently. IDP can detect these scans by counting the number of ports scanned in a specified time period. You can also set a session limit threshold, which defines the maximum number of sessions for a single host.
Detecting TCP and UDP Port Scans
To detect TCP and UDP port scans, set a port count (number of ports scanned) and the time threshold (the time period that ports are counted) in seconds.

Example: Traffic Anomalies Rule
You want to create a Traffic Anomalies rule that looks for port scans on your internal network. You set both the TCP and UDP Port Count to 20 and the Time threshold to 120 seconds. The rule is matched if the same Source IP scans 20 TCP ports on your internal network within 120 seconds, or if the same Source IP scans 20 UDP ports on your internal network within 120 seconds.

Detecting Other Scans
In addition to port scans, the attacks can occur over multiple connections and sessions:

- **Distributed Port Scans.** Use multiple Source IP addresses to scan ports.
- **ICMP Sweeps.** Use a single Source IP to ping multiple IP addresses.
- **Network Scans.** Use a single Source IP to scan multiple IP addresses.

To detect these attacks, set the IP Count (the number of times attempts to scan or ping ports on your network occur) and the Time (the time period that IP addresses are counted) in seconds.

Example: Traffic Anomalies Rule
To create a Traffic Anomalies rule that looks for distributed port scans on your internal network, set the IP Count to 50 and the Time to 120 seconds. If 50 IP addresses attempt to scan ports on your internal network within 120 seconds, the rule is matched.

Example: Traffic Anomalies Rule
You want to create a Traffic Anomalies rule that looks for network scans and ICMP sweeps on your internal network. You set the IP Count to 50 and the Time to 120 seconds for ICMP sweeps and network scans. The rule is matched if:

- The same Source IP attempts to scan 50 IP addresses on your internal network within 120 seconds
- The same Source IP attempts to ping 50 IP addresses on your internal network within 120 seconds

**NOTE:** Because a distributed port scan uses multiple source IP addresses, the source IP address appears as 0.0.0.0 in a scan log.
Session Limiting
You can set a session limit threshold that defines the maximum number of sessions allowed from a single host within a second. For each source IP specified in the rule, the Sensor tracks the sessions per second; if the session rate exceeds the user-defined maximum, the Sensor generates a SCAN_SESSION_RATE_EXCEEDED event log record, which appears in the Log Viewer. To take action when this event is triggered, configure an IP action in the rule.

**NOTE:** When you configure a Traffic Anomalies rule to block traffic that exceeds a specified session limit, the sessions counted are based on the source IP address only; the destination address and destination port values are set to 0. This means that if you set the Blocking Options for this rule to include the destination IP address or the destination port, IDP does not block traffic as there are no sessions that match the destination address 0 or the destination port 0. When configuring session limiting for a Traffic Anomalies rule, you should use Blocking Options that specify the source address only and not the destination address/port. For example, select “Source” or “Source, Protocol” from the Blocking Options.

Figure 90 shows options for setting a sessions threshold for a Traffic Anomalies rulebase.

**Figure 90: Setting the Session Limit Options**

![View Detect Options](image)
Example: Session Limiting

- Your internal network typically has a low volume traffic. To detect a sudden increase in traffic from a specific host (which might indicate a worm), set the source IP to your Internal Network and configure the session count as 200 session/sec. To block traffic that exceeds the session limit, set an IP action of IDP Block and choose Source, Protocol from the Blocking Options menu.

Adding the Traffic Anomalies Rulebase

Before you can configure a rule in the Traffic Anomalies rulebase, you need to add the Traffic Anomalies rulebase to a Security Policy.

1. In the main navigation tree, select Security Policies. Open a security policy by double-clicking the policy name in the Security Policies window or by clicking the policy name and then selecting the Edit icon.

2. Click the Add icon in the upper right corner of the Security Policy window and select Add Traffic Anomalies Rulebase to open the Traffic Anomalies rulebase tab.

3. To configure a Traffic Anomalies rule, click the Add icon on the left side of the Security Policy window to open a default Traffic Anomalies rule. You can modify this rule as needed.

Figure 91 shows a default Traffic Anomalies rulebase that has been modified.

Figure 91: Traffic Anomalies Rulebase

<table>
<thead>
<tr>
<th>No.</th>
<th>Match</th>
<th>Traffic Anomalies</th>
<th>IP Action</th>
<th>Notification</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>any</td>
<td>any</td>
<td>IP Block</td>
<td>Logging</td>
</tr>
</tbody>
</table>

Defining Match

You specify the traffic you want IDP to monitor for network anomalies.

Configuring Source & Destination Address Objects

Set the Source object to Any. Set the Destination Object to any Address Objects you want to protect.

Configuring Services

Set the Service to Any, unless you want to tailor different rules to different services.

Setting Detect Options

Right-click the rulebase cell in the Traffic Anomalies column and select Detect. In the View Detect Options dialog, set the Port Count and Time Threshold values for each value you want to monitor. The values are measured in number of hits (Port Count) in a particular number of seconds (Time Threshold).
Setting Response Options

The IP Action column governs what action the IDP Sensor takes when it finds a matching condition.

Right-click the rulebase cell in the IP Action column and select Configure. The Configure IP Action dialog displays.

Configure your IP Action settings as appropriate for your network. Figure 92 shows options for configuring IP action.

Figure 92: Configuring IP Action

Setting Notification

You can choose to log an attack and create log records with attack information that you can view real-time in the Log Viewer. For more critical attacks, you can also set an alert flag to appear in the log record.

To log an attack for a rule, right-click the Notification column of the rule and select Configure. The Configure Notification dialog box appears.

The first time you design a Security Policy, you might be tempted to log all attacks and let the policy run indefinitely. Don’t do this! Some attack objects are informational only, and others can generate false positives and redundant logs. If you become overloaded with data, you can miss something important. Remember that Security Policies that generate too many log records are hazardous to the security of your network, as you might discover an attack too late or miss a security breach entirely due to sifting through hundreds of log records. Excessive logging can also affect IDP throughput, performance, and available disk space. A good Security Policy generates enough logs to fully document only the important security events on your network.

Setting Logging

In the Configure Notification dialog box, select Logging and then click OK. Each time the rule is matched, the IDP system creates a log record that appears in the Log Viewer.
You can choose to log an attack and create log records with attack information that you can view real-time in the Log Viewer. For more critical attacks, however, you might want to be notified immediately by email, have IDP run a script in response to the attack, or set an alarm flag to appear in the log record. Your goal is to fine-tune the attack notifications in your Security Policy to your individual security needs.

Setting an Alert
In the Configure Notification dialog box, select Alert and then click OK. If Alert is selected and the rule is matched, IDP places an alert flag in the alert column of the Log Viewer for the matching log record.

Logging Packets
You can record the individual packets in the network traffic that matched a rule by capturing the packet data for the attack. Viewing the packets used in an attack on your network can help you determine the extent of the attempted attack and its purpose, whether or not the attack was successful, and any possible damage to your network.

---

NOTE: To improve IDP performance, log only the packets after the attack.

If multiple rules with packet capture enabled match the same attack, IDP captures the maximum specified number of packets. For example, you configure Rule 1 to capture 10 packets before and after the attack, and Rule 2 to capture 5 packets before and after the attack. If both rules match the same attack, IDP attempts to capture 10 packets before and after the attack.

NOTE: Packet captures are restricted to 256 packets before and after the attack.

---

Setting Severity
You can override the inherent attack severity on a per-rule basis within the SYN Protector rulebase. You can set the severity to either Default, Info, Warning, Minor, Major, or Critical.

To change the severity for a rule, right-click the Severity column of the rule and select a severity.

Specifying VLANs
You can specify that the rule be applied only to packets from particular VLANs. See Setting VLAN Tags for IDP Rules on page 361 for more information.

Setting Target Devices
For each rule in the rulebase, you can select the IDP-capable device that will use that rule to detect and prevent attacks. Alternatively, you can use Device Manager to assign policies to devices.
Entering Comments

You can enter notations about the rule in the Comments column. Anything you enter in the Comments column is not pushed to the target device(s). To enter a comment, right-click the Comments column and select Edit Comments. The Edit Comments dialog box appears. You can enter up to 1024 characters in the Comments field.

Configuring Network Honeypot Rules

The Network Honeypot protects your network by impersonating open ports on existing servers on your network, alerting you to attackers performing port scans and other information-gathering activities.

NOTE: The Network Honeypot Rulebase is a terminal rulebase; when IDP finds a match on a rule, it does not execute succeeding rules.

Impersonating a Port

Attackers view ports as entry points into your network. You can create counterfeit ports on existing servers to trick attackers who are attempting to break into your network. A counterfeit port can appear to offer notoriously vulnerable services to make the port attractive to attackers.

- You create a counterfeit port in the Network Honeypot Rulebase by specifying an existing Network Object and choosing a port and service to impersonate. You can also set an IP Action to perform against the Source IP. If an attacker attempts to communicate with your counterfeit port, the rule matches and the IP action triggers.

Adding the Network Honeypot Rulebase

Before you can configure a rule in the Network Honeypot rulebase, you need to add the Network Honeypot rulebase to a Security Policy.

1. In the main navigation tree, select Security Policies. Open a security policy by double-clicking the policy name in the Security Policies window or click the policy name and then select the Edit icon.

2. Click the Add icon in the upper right corner of the Security Policy window and select Add Network Honeypot Rulebase. The Network Honeypot rulebase tab appears.

3. To configure a Network Honeypot rule, click the Add icon on the left side of the Security Policy window. A default Network Honeypot rule appears. You can modify this rule as needed.

Figure 93 shows a default Network Honeypot rulebase that has been modified.
Defining Match

You specify the traffic you want IDP to monitor for network anomalies.

Configuring Source

Set the Source object to Any.

Configuring Destination Address Objects and Services

Set the Destination Address and Service to the service that will appear to be available on the indicated address object.

Setting Operation

Right-click the cell in the Operation column and select Impersonate. This tells the IDP Sensor to impersonate the indicated services on the indicated device.

Setting Response Options

The IP Action column governs what action the IDP Sensor takes when it finds a matching condition.

Right-click the rulebase cell in the IP Action column and select Configure. The Configure IP Action dialog displays.

Configure your IP Action settings as appropriate for your network.

Setting Notification

You can choose to log an attack and create log records with attack information that you can view real-time in the Log Viewer. For more critical attacks, you can also set an alert flag to appear in the log record.

To log an attack for a rule, right-click the Notification column of the rule and select Configure. The Configure Notification dialog box appears.

Setting Logging

In the Configure Notification dialog box, select Logging and then click OK. Each time the rule is matched, the IDP system creates a log record that appears in the Log Viewer.
You can choose to log an attack and create log records with attack information that you can view real-time in the Log Viewer. For more critical attacks, however, you might want to be notified immediately by email, have IDP run a script in response to the attack, or set an alarm flag to appear in the log record. Your goal is to fine-tune the attack notifications in your Security Policy to your individual security needs.

Setting an Alert

In the Configure Notification dialog box, select Alert and then click OK. If Alert is selected and the rule is matched, IDP places an alert flag in the alert column of the Log Viewer for the matching log record.

Logging Packets

You can record the individual packets in the network traffic that matched a rule by capturing the packet data for the attack. Viewing the packets used in an attack on your network can help you determine the extent of the attempted attack and its purpose, whether or not the attack was successful, and any possible damage to your network.

NOTE: To improve IDP performance, log only the packets after the attack.

If multiple rules with packet capture enabled match the same attack, IDP captures the maximum specified number of packets. For example, you configure Rule 1 to capture 10 packets before and after the attack, and Rule 2 to capture 5 packets before and after the attack. If both rules match the same attack, IDP attempts to capture 10 packets before and after the attack.

NOTE: Packet captures are restricted to 256 packets before and after the attack.

Setting Severity

You can override the inherent attack severity on a per-rule basis within the SYN Protector rulebase. You can set the severity to either Default, Info, Warning, Minor, Major, or Critical.

To change the severity for a rule, right-click the Severity column of the rule and select a severity.

Specifying VLANs

You can specify that the rule be applied only to packets from particular VLANs. See Setting VLAN Tags for IDP Rules on page 361 for more information.

Setting Target Devices

For each rule in the rulebase, you can select the IDP-capable device that will use that rule to detect and prevent attacks. Alternatively, you can use Device Manager to assign policies to devices.
Entering Comments
You can enter notations about the rule in the Comments column. Anything you enter in the Comments column is not pushed to the target device(s). To enter a comment, right-click the Comments column and select Edit Comments. The Edit Comments dialog box appears. You can enter up to 1024 characters in the Comments field.

Installing Security Policies
After you have successfully verified your Security Policy, you must:
1. Assign the policy to your managed devices
2. Validate the policy
3. Install the policy on your managed devices
The following sections detail each step.

Assigning a Security Policy to a Device
New devices do not have an existing or default Security Policy. However, when you import a device configuration, NetScreen-Security Manager automatically imports all existing policies for the device. To simplify policy management, you can merge these multiple device policies into a single Security Policy that you install on several devices at one time. For details, see “Merging Policies” on page 396.

After you have created a Security Policy, you must assign that policy to a device. Assigning a policy to a device links the device to that policy, enabling NetScreen-Security Manager to install the policy on that device. To assign an existing policy to a device, use one of the following methods:

- Right-click a device and select Policy > Assign Policy. Select the policy you want to assign to the device.
- Double-click a device to open the device configuration. In the Info tab, under Policy for device, select the policy you want to assign to the device.

You can use a single Security Policy to control multiple security devices. Each rule in a Security Policy contains an Install On column that specifies the devices the rule is applied to. This means that you can assign a Security Policy to a device, but only some of the rules in that policy are actually installed on that device during a device update.

You can also create multiple policies for a single device, but only one Security Policy can be active on the device. When you update a device configuration, NetScreen-Security Manager installs the active policy on the security device. By default, NetScreen-Security Manager considers the active policy as the policy that was most recently edited.

NOTE: If you delete and then re-import a device, you must reassign a policy to the device.
Validating Security Policies

You should validate a Security Policy to identify potential problems before you install it. NetScreen-Security Manager contains a Policy Validation tool to help you locate common problems, such as:

- **Rule Duplication**—Occurs when one or more rules in the Security Policy are identical. For more information, see “Rule Duplication” on this page.

- **Zone Mismatch**—Occurs when the source or destination zone you have chosen in a rule is not available on the device you selected in the Install column.

- **Rule Shadowing**—Occurs when a strict rule has no effect on traffic because it follows a broader rule. For more information, see “Rule Shadowing” on page 387.

- **Unsupported Options**—Occurs when a device in the Install column of a rule does not support a specific rule option configured for the rule. For details, see “Unsupported Options” on page 387.

To use the Policy Validation tool to validate a Security Policy, you must first assign the Security Policy to a device. Then, to validate a policy, from the menu bar click **Devices > Policy > Validate Policy**. A Job Manager window appears to display job information and progress. Policy validation analyzes the source and destination addresses, the to and from zones, and the service when validating. If NetScreen-Security Manager identifies any problems in the policy during policy validation, it displays information about the problem at the bottom of the selected rulebase.

---

**NOTE:** We highly recommend that you validate a policy before installing it. A Security Policy that has internal problems can leave your network vulnerable.

---

**Rule Duplication**

Rule duplication occurs when an administrator configures the same rule in a rulebase more than once. Rule duplication can also occur during the rule validation process for devices running ScreenOS 4.0.x. For ScreenOS 4.0.x, NSM treats each element of the rule as a separate rule. For example, when a rule with two service objects (AOL and DNS) is sent to the device, NSM sends it as two rules, one rule with AOL and another with DNS.

**NOTE:** For ScreenOS 5.x, NSM sends rules with multiple objects or elements. For example, NSM can send a rule with two or more service objects as one rule.

You should delete all duplicate rules to maintain policy lookup efficiency.

Figure 94 shows an example of rule duplication. If NSM sends these two rules to a device running ScreenOS 4.x, rule validation fails because Rule 2 is duplicated in Rule 1 (the device receives two exactly matching rules from the same source/destination that use HTTP service). A ScreenOS 5.x device passes the policy validation process for HTTP; however, Rule 2 is not needed. To correct this problem, you should delete Rule 2.
Rule Shadowing

Rule shadowing occurs when an administrator selects or configures a policy in such a way that the next rules have no effect on traffic. Rule shadowing can introduce system vulnerabilities and packet dropping. Policy validation identifies rule shadowing. You should modify or delete all rules that overshadow others.

When a packet comes in, a security device compares it to the first rule in the policy. If a match occurs, the device executes the action associated with the rule. If no match occurs, the rule has no effect. Then, the device compares the packet to the next rule in the policy (unless the prior rule was a “terminal” rule.) So, each packet gets compared to every rule in the policy until a match occurs or a terminal rule ends the match process.

For example, if Rule 1 is a terminal rule, and a packet matches Rule 1, then the device will never compare the packet to the next rule(s). Or, if Rule 1 causes the packet to be dropped, and Rule 2 adds a diffserv marking, the diffserv marking will never be added.

In Table 31 Rule 1 shadows Rule 2. Rule 1 allows any service to a web server, but Rule 2 denies the service HTTP. When the security device receives a packet requesting HTTP service with the web server, Rule 1 allows the traffic. Rule 2 which denies HTTP is never checked.

Table 31: Rule Shadowing Example

<table>
<thead>
<tr>
<th>Rule</th>
<th>From Zone</th>
<th>Source</th>
<th>To Zone</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Untrust</td>
<td>Any</td>
<td>DMZ</td>
<td>Web server</td>
<td>Any</td>
<td>Allow</td>
</tr>
<tr>
<td>2</td>
<td>Untrust</td>
<td>Any</td>
<td>DMZ</td>
<td>Web server</td>
<td>HTTP</td>
<td>Deny</td>
</tr>
</tbody>
</table>

Unsupported Options

Policy Validation can also identify unsupported options in your Security Policy. Because different security 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).
- Destination NAT Option not available on 4.0.x devices.
Installing New Security Policies

Before you install a new Security Policy, ensure that you have:

- **Assigned the policy to your devices**—After you have created a Security Policy, you must assign that policy to the devices you want to use that policy. Assigning a policy to a device links the device to that policy, enabling NetScreen-Security Manager to install the policy on that device.

- **Selected the correct devices for the Install On column of each rule**—A security device can only use one Security Policy at a time; when you install a new policy, it overwrites all existing policies on the security device.

- **Configured each device in the Install On column of each rule correctly**—When you push a policy to a device, you also push the device configuration to the device. Any changes made (by you or another admin) to the device configuration are pushed to the device along with the policy.

- **Configured rules in each rulebase correctly**—The management system installs rules from all rulebases on the specified device. For information about rule installation and rule execution sequence, see “Rule Execution Sequence” on page 322.

- **Configured the VPN rules or VPN links in the policy correctly**—The management system installs all VPN rules in the policy.

Additionally, to help you identify possible problems in your policy, you might want to run a Delta Config Summary before pushing the policy.
During policy installation, NetScreen-Security Manager installs the rules in the policy on the security devices you selected in the Install On column of each rule. The install process occurs between the management system and your managed devices. First, the GUI Server creates the ADM file that contains all policies for all devices selected for update (although the ADM file collects information from all policies, it does not merge the policies) The GUI Server sends the ADM to the Device Server. Next, the NetScreen-Security Manager Device Server receives the ADM and uses it to create a separate, individual DM for each device that you selected for update:

- For 5.x devices, the Device Server sends the DM to the managed device, which translates the information in the DM into commands and runs those commands on the devices.
- For 4.0.x devices and earlier, the Device Server translates the DM into commands and send those commands to the managed device, which runs those commands.

For information about the device ADM and DM, see the “Managing Device Capabilities” on page 214.

**Configuring IDP Policy Push Timeout**

IDP policies, due to their possibly large number of attack objects, may take a long time to upload and compile. The default timeout for IDP policy is 40 minutes, but you can set it higher if your policy uploads are timing out. Usually, this will only occur the first time a policy is pushed to a newly deployed Sensor.

To set the timeout to a higher value, edit the following file:

```
/usr/netscreen/DevSvr/var/devSvr.cfg
```

Change the following setting:

```
devSvrDirectiveHandler.idpPolicyPush.timeout 2400000
```

The setting is measured in milliseconds (1000's of a second). So, 2400000 milliseconds is equal to 40 minutes.
Updating Existing Security Policies

To install a new or modified policy on a managed device, from the toolbar, select Devices > Configuration > Update Device Config. If you changed the device configuration or assigned policy for a device, that device is automatically selected. Unselect any devices you do not want to update.

You can also enable session rematch for policy installations on managed devices running ScreenOS 5.1 or higher. Session rematch enables NetScreen-Security Manager to preserve the existing sessions that are being tracked by the installed Security Policy during the policy update procedure. At the end of the update, NetScreen-Security Manager restores all valid sessions on the managed device and deletes all invalid sessions (a session is considered valid when the From Zone, Source, To Zone, Destination, and Service of the traffic is the same before and after the new policy installation).

You enable session rematch when you update devices (from the menu bar, select Devices > Configuration > Update Device Config). To enable session rematch from the Update Devices dialog box, select Options, then select Rematch, session treatment when modifying a policy rule, then click OK.

NOTE: You can also enable/disable session rematch in the system-wide device update settings. To configure, from the menu bar, select Tools > Preferences > Device Update. The system-wide setting (enabled or disabled) becomes the default setting for all device updates, but you can change the setting as needed for each individual update.

After you have selected the devices you want to update (and configured session rematch, if desired), click OK to begin the update process. The Job Manager dialog box appears and displays the progress of the policy installation. As the update is performed, the main display area of the Job Manager dialog box displays the CLI commands that the management system is sending to the physical device. In some cases, you might see that the policy is unset, then reset on the device.

NetScreen-Security Manager does not need to reset the policy when:

- The Security Policy you are installing does not exist on the physical device. The update installs the Security Policy on the device.

- The Security Policy you are installing already exists on the physical device. The update modifies the policy on the physical device, without resetting the policy.

NetScreen-Security Manager must reset the policy when the Security Policy you are installing already exists on the physical device, but an object within the policy has changed in NetScreen-Security Manager. The update first unsets the current policy on the device, deletes the old object, adds the new changed object, then installs the entire Security Policy again on the physical device.

NOTE: Additionally, NetScreen-Security Manager must reset the policy during an import when the Security Policy exists on the device, but does not exist in the management system.
After the updated has completed, close the Job Manager window. The rules in the policy become active on the devices you selected in the Install On column of the rule. To see the exact rules that were applied to a specific device, in Device Manager, right-click a device and select Policy > View Pending Device Policy.

Updating Only the IDP Rulebases on ISG Devices
On ISG devices with IDP, you can elect to push only the IDP rulebases, not the entire policy.

To push only the IDP rulebases, not the firewall or multicast rulebases, select the Update IDP Rulebase Only checkbox in the Update Device Options dialog.

The IDP-on-ISG rulebases are as follows:

- IDP
- Backdoor
- Exempt.

Managing Rules and Policies

Managing rules and policies for multiple security devices can seem daunting at first. Take some time to carefully design your policies to make them efficient.

- Helpful Tips
- Using Zone Exceptions
- Selecting Rules
- Editing Rule Order
- Using Cut, Copy, and Paste
- Deleting a Rule
- Disabling a Rule
- Using Rule Groups
- Re-Importing Devices & Security Policies
- Merging Policies
- Exporting Policies

Helpful Tips

Some helpful tips about managing your rules and policies:

- Because a device can have only one Security Policy installed at a time, you must include all rules for that device in one policy.

Each Security Policy contains a default firewall rulebase (Zone); you can add other rulebases (Global, Multicast, IDP, Exempt, Backdoor) to create additional rules.

Each rulebase can contain one or more rules, up to 40,000 max for the Security Policy. The top rule in the rulebase is rule 1, and second rule is rule 2, and so on. To combine rules for easier management within the Zone rulebase, you can create rule groups.

Each rule group can contain one or more rules, up to 40,000 max for the Security Policy. Rules within a rule group follow the rulebase numbering sequence.

The IDP, Exempt, or Backdoor rulebases are not included when you:

- Merge two policies into a single policy
- Import a Security Policy from an existing IDP-capable security device

You cannot disable an entire Security Policy or a rulebase. You can, however, disable individual rules; for details, see “Disabling a Rule” on page 395.

When you re-import a device that was previously managed by NetScreen-Security Manager, you must manually re-assign a policy to a re-imported device. For information about re-importing issues, see “Re-Importing Devices & Security Policies” on page 395.

Using Zone Exceptions

A zone exception is a powerful tool that can help reduce the number of rules in your Security Policy while maintaining the same functionality. Zone exceptions add flexibility to your rules, enabling you to include more devices in a single rule. You can add multiple zone exceptions for the To Zone or From Zone of a rule in the Zone rulebase.

To configure a zone exception, in the To Zone or From Zone column of a rule, right-click and select Select Zone Exception. Configure a zone and the device on which that zone is configured. When you update your managed devices with the Security Policy and the rule is installed on the security device, the zone exception for that device appears as the designated To Zone or From zone.

EXAMPLE: USING ZONE EXCEPTIONS

In this example, you want to configure a rule in your Security Policy that controls all traffic from the trust zone to the untrust zone on two security devices. However, one device, the NS-208A, contains a DMZ zone through which all traffic from trust and untrust zones must pass. Using a zone exception, you enable the NS-208A to use the DMZ zone instead of the trust zone as the From Zone value.

To configure this zone exception in a rule:
1. In the main navigation tree, select Security Policies. In the main display area, click the Add icon to display the New Security Policy dialog box. Enter a name for the policy, click OK, then select the policy in the main navigation tree.

2. Modify the default rule:

   - In the Action column, right-click and select Permit.
   - In the Install On column, right-click and select the Corsica and NS-208A security devices.

3. Configure the zone exception:

   a. In the From Zone column of the rule, right-click and select Select Zone Exceptions. The Zone Exceptions dialog box appears.
   b. Click the Add icon to display the New Zone Exceptions dialog box. Configure as shown below, then click OK:

   Figure 97: Zone Exceptions Example

   - For Zone, select dmz.
   - For Device, select the NS-208A security device.
   c. Click OK again to save the zone exception to the rule, which now appears as shown below:

   Figure 98: Zone Exceptions Example Rule

   Selecting Rules

   To select a single rule, click anywhere in the rule. The following sections explain how to:

   - Editing Rule Order
   - Using Cut, Copy, and Paste
Deleting a Rule
Disabling a Rule
Using Rule Groups

Editing Rule Order
To change the order of rules in a policy, right the No. Column (the first column) of a rule and select Move Rule Up or Move Rule Down.

Using Cut, Copy, and Paste
To quickly create multiple rules that use the same basic information, copy and paste the rule, then change the parameters in each copied rule to make the rule unique (this is especially useful for rules that contain detailed rule options such as attack protection).

NOTE: When you cut and paste a rule, your preferred ID is retained. However, when you copy and paste a rule, a new ID is created.

To cut and paste a rule, right-click inside the No. column (the first column) of the rule and select Edit > Cut. Next, select a rule that is above or below the position you want to paste the cut rule into, then select Edit > Paste > <above> <below>.

NOTE: The cut rule remains visible in its original position until you paste it into its new position.

Dragging and Dropping Objects
Use the pull-down menu in the “Shared Objects For” pane to easily select and add shared objects including address, service, Global MIP, Global VIP, attack, device, VLAN or custom field objects to your security policies. After selecting the object you want, simply drag and drop them into the appropriate policy column.

NOTE: You can not drag and drop objects into a column that is not appropriate for that object. For example, you can not drop a service object into the “Install On” column; you can not drop a standalone IDP device into the “Install On” column for a zone-based firewall rulebase. Dragging and dropping objects is also not supported on any Predefined IDP policy.

Deleting a Rule
To delete a rule, right-click inside the No. column (the first column) of the rule and select Delete. You can also delete a rule group; however, deleting the rule group also deletes all rules within the rule group.
Disabling a Rule
To disable a rule, right-click inside the No. column (the first column) of the rule and select Disable. The rule remains in the rulebase, but displays a gray diagonal stripe to indicate that it has been disabled. While the rule is disabled, NetScreen-Security Manager does not install the rule on any devices.

To enable a rule, right-click inside the No. column (the first column) of the rule and select Disable again to clear the checkbox. You can disable rule groups using the same method.

Using Rule Groups
To create a rule group, select the rules you want to include in the group, then right-click and select create rule group. Enter a name and description for the rule group, then click OK.

Combining rules into a rule group can help you better manage rules. For example, you might want to create rule group for:

- VPN rules or VPN links
- Rules that manage traffic from a specific zone or interface on the security device
- Rules for a specific device or device group
- Rules that provide attack or AV protection
- Rules that manage VoIP traffic with GTP objects

You can add, edit, and delete rule groups; however, deleting a rule group also deletes all rules within that group. If necessary, you can also ungroup a rule group.

You can create multiple rule groups (40,000 rules max in a Security Policy). NetScreen-Security Manager supports one level of rule groups; you cannot create a rule group within a rule group.

Re-Importing Devices & Security Policies
Occasionally, you might need to delete and then re-add a security device to NetScreen-Security Manager. After you re-import the device configuration for a device that was previously managed by NetScreen-Security Manager:

- If you made no changes to the device policies using the WebUI or CLI, when you re-import the device, NetScreen-Security Manager does not create a new Security Policy.
- If you made changes to the devices policies using the WebUI or CLI, when you re-import the device, NetScreen-Security Manager creates a new Security Policy.
You must manually re-assign a policy to a re-imported device. For example, if you re-import a previously-managed security device, you might want to first merge the imported policy with a more comprehensive policy, then assign the comprehensive policy to the device.

**NOTE:** Importing the running configuration from a device completely overwrites all configuration information stored within NetScreen-Security Manager for that device. To help avoid accidental configuration overwriting, when you attempt to import a configuration from a currently managed security device, NetScreen-Security Manager prompts you for confirmation to import.

### Merging Policies

When you import policies from a single managed device, those policies appear in NetScreen-Security Manager as rules in a new policy. Each device policy is imported as a single rule, and the rules make up the policy that exists on the device.

**NOTE:** In the ScreenOS WebUI and CLI, a Security Policy is a single statement that defines a source, destination, zone, direction, and service. In NetScreen-Security Manager, those same statements are known as rules, and a Security Policy is a collection of rules.

To simplify policy management and maintenance, you can merge two policies into a single Security Policy. To merge two policies, select a source policy and a target policy:

- The source policy contains the rules that you want to merge into another policy (in the UI, this is the From Policy).
- The target policy receives the rules from the source policy (in the UI, this is the To Policy).

NetScreen-Security Manager copies the rules from the source policy and pastes them above, below, or inline with the rules in the target policy. When placing rules inline, be aware of the intra-policy dependence of both policies. Because rule order is important (rules are executed top-down), rules can be dependant on other rules. If you rearrange the order of dependant rules by inserting merged rules, the security device changes the way it handles the packets. If you are unsure if you have intra-policy dependence in your rules, it’s best to merge rules above or below the existing rules.

After creating a single Security Policy that contains both source and target rules, NetScreen-Security Manager also identifies rules that contain similar values in the source, destination, service, and install on columns, then collapses those rules into a single rule. NetScreen-Security Manager does not collapse rules that contain different zones, or rules that refer to unique VPNs.

By default, NetScreen-Security Manager also updates the device policy pointers to reference the new merged policy (the device policy pointer indicates which Security Policy is assigned to a device). When configuring Policy Merge settings, you can edit this option to keep the device policy pointers for both the source and target policies.
You can merge any two Security Policies. To access the Policy Merge tool, select the Security Policies, then use the menu bar to select Tools > Policy Merge. See the NetScreen-Security Manager Online Help for details.

NOTE: You can merge rules from 4.0.x or 5.0.x devices that use the deny action into rules from 5.1 or higher devices that use the reject action, provided that the source, destination, source, and service are the same for the rules. NetScreen-Security Manager automatically subsumes the deny action into the reject action for rules imported or merged from 4.0.x and 5.0.x devices; when the merged Security Policy is installed on the device however, the action appears as deny for 4.0.x and 5.0.x devices and as reject for 5.1 and higher devices.

EXAMPLE: MERGING SECURITY POLICIES
Policy A contains the following rules:

Figure 99: Security Policy A Rules (Before Policy Merge)

<table>
<thead>
<tr>
<th>No.</th>
<th>ID</th>
<th>Match From Zone</th>
<th>Source</th>
<th>To Zone</th>
<th>Service</th>
<th>Action</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>trust</td>
<td>1.1.1.1</td>
<td>untrust</td>
<td>2.2.2.2</td>
<td>FTP</td>
<td>permit</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>trust</td>
<td>3.3.3</td>
<td>untrust</td>
<td>4.4.4.4</td>
<td>HTTP</td>
<td>permit</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>trust</td>
<td>5.5.5</td>
<td>untrust</td>
<td>6.6.6.6</td>
<td>ICMP-ANY</td>
<td>permit</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>TELNET</td>
<td>Bozeman</td>
</tr>
</tbody>
</table>

Policy B contains the following rules:

Figure 100: Security Policy B Rules (Before Policy Merge)

<table>
<thead>
<tr>
<th>No.</th>
<th>ID</th>
<th>Match From Zone</th>
<th>Source</th>
<th>To Zone</th>
<th>Service</th>
<th>Action</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>trust</td>
<td>1.1.1.1</td>
<td>untrust</td>
<td>2.2.2.2</td>
<td>FTP</td>
<td>permit</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>trust</td>
<td>3.3.3</td>
<td>untrust</td>
<td>4.4.4.4</td>
<td>HTTP</td>
<td>permit</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>trust</td>
<td>5.5.5</td>
<td>untrust</td>
<td>6.6.6.6</td>
<td>ICMP-ANY</td>
<td>permit</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>TELNET</td>
<td>Tokyo</td>
</tr>
</tbody>
</table>

To merge Policy A (from policy) with Policy B (to policy), from the file menu, select Tools > Policy Merge Tool and configure the merge as shown below:
Managing Rules and Policies

NetScreen-Security Manager copies all rules from Policy A and pastes them above the rules in Policy B. Next, NetScreen-Security Manager merges the matching values in the columns to create a single, simplified policy (Policy C):

**Figure 101: Configure Policy Merge**

![Policy Merge Tool](image)

NetScreen-Security Manager copies all rules from Policy A and pastes them above the rules in Policy B. Next, NetScreen-Security Manager merges the matching values in the columns to create a single, simplified policy (Policy C):

**Figure 102: Security Policy Rules (Merged from Policy A and Policy B)**

<table>
<thead>
<tr>
<th>No.</th>
<th>ID</th>
<th>Match</th>
<th>Action</th>
<th>Instal On</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>From Zone</td>
<td>Source</td>
<td>To Zone</td>
</tr>
<tr>
<td>1</td>
<td>3</td>
<td>trust</td>
<td>3.3.3.3</td>
<td>untrust</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>trust</td>
<td>1.1.1.1</td>
<td>untrust</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>trust</td>
<td>5.5.5.5</td>
<td>untrust</td>
</tr>
<tr>
<td>4</td>
<td>3</td>
<td>trust</td>
<td>3.3.3.3</td>
<td>untrust</td>
</tr>
</tbody>
</table>
Exporting Policies

You can export a security policy rulebase to an HTML file.

To export a security policy, select File > Export Policy. (You can also use the button or Alt-E.) In the Export Policy dialog box, select the rulebases you wish to export. Indicate whether you want to display expanded rule groups and whether you want to see the expanded view. Click the Browse button to select a default export directory for all future exports. Click Export to export the file.

Each export creates a new directory. The default directory name is `<policyname>_YYMMDD_HHMMSS`. The export process puts each rulebase in a separate HTML file in that directory.

Use an HTML browser to view the exported file. Expanded views may make the output too wide for a standard printer.

Example: Exporting Zone Based Firewall Rules with Expanded View
To export an expanded view of the Zone based Firewall Rules from a security policy, select a policy from Security Policies. Then select File > Export Policy from the menu bar. In the dialog box, select Zone based Firewall Rules. Select Show Expanded View. Browse to an export directory and click Select Export Directory. Click Export.

Figure 103: Export Policy Dialog with Options Selected

NetScreen-Security Manager creates a new subdirectory for each export. To view the policy, point your browser at the file zone.html in the created subdirectory.
Pre/Post Rules

In NSM, a policy supports many kinds of rulebases. Each rulebase is an ordered list of rules. Pre rules and post rule are also ordered lists of rules that are defined from the Central Manager at the global domain and sub-domain levels as well as on regional servers in standalone NSM installations. You can define and apply pre/post rules for each rulebase type.

When you update a device, device-specific policy configurations are generated for the device. This creates rulebases by applying the following rules in the following order (from first to last):

- Pre rules
- Policy rulebase rules
- Post rules

The pre/post rules feature provides a policy definition at a domain level that can be applied to all devices within the specific domain and all subdomains. Users can define two sets of rules for any rulebase type that can be applied as pre and/or post rules for any device of the given domain and subdomains.

Pre/post rules are two sets of rules of any rulebase type that can be created for any domain. Configuration of pre/post rules are located in the main navigational tree under Policy Manager called Central Manager Policies. Domain Administrators can edit domain level policies from this option.

Pre rules apply before any rules of a rulebase are applied to a device and post rules apply after any rules of a rulebase are applied to a device. Pre and post rules in the integrated view are not editable. There is only one instance of pre/post rules for a specific domain.

Domain hierarchy is used when applying pre/post rules to subdomains. Within any subdomain, global domain pre rules take precedence over subdomain pre rules, which take precedence over Security policy specific rules. Similarly, Security policy rules take precedence over subdomain post rules, which take precedence over global domain post rules.

All features of Security Policies are available for pre and post rules.

- **Import device command**—imports all rules into the security policy that is created for the device.
- **Config summary**—displays the pre and post rules.
- **View device pending policy**—displays the policy being pushed to a device including pre and post rules from current and parent domains.
- **Validate policy**—validates policy rules.

NOTE: The Central Manager attack database version must match the regional server attack database version to push pre/post rules.
- **View domain rules**—When checked, any predefined or custom policy displays the pre/post rules above and below the policy rules. These rules are displayed in a different color and not editable. (See Figure 104 below.)

Pre/post rules can include rulegroups. The firewall rulebase for pre/post rules cannot contain VPN rules or VPN links.

![Figure 104: Pre/Post Rules](image)

When the regional server pushes a rulebase to a device that is not contained within the regular policy, a warning message is displayed in the **Job Manager** window notifying the user that a rulebase was pushed that is not contained within the regular policy.

**Rule Application Sequence**

Since pre/post rules are defined at the Central Manager, global, and sub-domain levels, NSM imposes a rule application precedence. When all pre/post rules are defined, the application order of rules in a rulebase are applied in the following order (from first to last):

- Central Manager pre rules
- Global domain pre rules
Sub domain pre rules
Specific rulebase rules the device uses
Sub domain post rules
Global domain post rules
Central Manager post rules

ScreenOS Devices
ScreenOS devices require rules to have unique IDs. Rules pushed to devices are the merged result of pre/post rules based on pre/post policy and local policy from the device. Enforcing uniqueness at the single policy level is not sufficient.

With the Central Manager pre/post rules, NSM enforces the uniqueness of a device rule’s preferred ID server-wide. Therefore, when an admin adds a domain level pre/post rule either from the regional server or from the Central Manager server pushing pre/post rules to the regional server, the regional server generates a server-wide unique preferred ID for the new rule. There is a preset ID range for firewall rulebases.

Validation of Pre/ Post Rules
In Central Manager servers, pre/post rules are validated the same way as rules validated in NSM policy manager. Central Manager pushes pre/post rules to the regional server and fills mapping tables with polymorphic objects. (See “Polymorphic Objects Overview” on page 222 for more details.) Invalid pre/post rules in the regional server are removed when the policy is pushed to a device during the device update operation.

Install-On Column for Pre/ Post Rules
In 2007.2 NSM Policy Manager, Install-On Column is the mechanism to specify which devices use a particular rule. While configuring a pre/post rule in Central Manager, rule application is applied at regional server level. Install-On Column, in this case, accepts only the Regional Server Object or ANY as legal entries. When a Central Manager pushes a pre/post rule to a regional server, content in this column specifies which rule is pushed to which regional server.

Managing Pre/ Post Rules
To manage post/pre rules, Central Manager admins can:

- Add Pre/Post Rules
- Push Pre/Post Rules to Regional Server
- Modify Pre/Post Rules
- Delete Pre/Post Rules
Add Pre/ Post Rules
This procedure assumes that a Central Manager admin is logged onto a Central Manager client.

To add a pre/post rule:

1. In the main navigation tree, select Policy Manager > Central Manager Policies.

2. Select either Central Manager Pre Rules or Central Manager Post Rules.

3. Click the Add icon in the toolbar and select Add Rule.

4. Select a regional server object for the rule’s Install On column, as necessary.

Pre/post rules can be added at the subdomain, global or central manager level.
Pre/post rules use the precedence of central manager, global and then sub-domain when applied to a policy.

Push Pre/ Post Rules to Regional Server

This procedure assumes that a Central Manager admin is logged onto a Central Manager client, and a pre/post rule has been added.

To push a pre/post rule:

1. In the main navigation tree, select Policy Manager > Central Manager Policies.
2. Select either Central Manager Pre Rules or Central Manager Post Rules.
4. Select the regional servers to which you want to push pre/post rules.

Central Manager Admin monitors progress from the Job Manager.
Pre/post rules and their referenced shared objects are replicated in the regional server(s) managed by Central Manager. The status and time of the pre/post rules push is clearly marked when an admin is logged onto a regional server.

Modify Pre/Post Rules

This procedure assumes that a Central Manager admin is logged onto a Central Manager client, and a pre/post rule has been pushed to a regional server.

To modify a pre/post rule:

1. In the main navigation tree, select **Policy Manager > Central Manager Policies**.

2. Select either **Central Manager Pre Rules** or **Central Manager Post Rules**.

3. Right-click the rule you want to modify and select **Copy**, **Paste**, or **Cut**. If you select **Paste**, you have additional options to paste the rule before or after another rule.

A modified pre/post rule replaces the existing pre/post rule on the regional server. Associated shared objects, if they are new, are replicated in the regional server.
Delete Pre/Post Rules

This procedure assumes that a Central Manager admin is logged onto a Central Manager client, and a pre/post rule has been pushed to a regional server.

To delete a pre/post rule:

1. In the main navigation tree, select **Policy Manager > Central Manager Policies**.
2. Select either **Central Manager Pre Rules** or **Central Manager Post Rules**.
3. Right-click the rule you want to modify and select **Delete**.

Associated shared objects (if they are not polymorphic objects), in the regional server, are also deleted from the regional server.
Polymorphic Objects

The Policy Manager uses shared objects (such as address, zone, and attack) when defining various components of a policy rule. Polymorphic objects are objects that can be defined at the Central Manager or regional server level. Polymorphic objects can be used as place holders for values that will be defined in a different context (in a regional server domain or subdomain, for instance).

Pre/post rules are defined at the Central Manager level or regional server level and can use shared objects that are defined by regional admins. To provide regional server admins the capability of customizing Central Manager pre/post rules, shared objects defined in Central Manager are flexible and customizable by regional admins, creating polymorphic objects.

Customizing Polymorphic Objects

Each polymorphic object contains a mapping table. Each entry of the mapping table has an attribute of domain, device, and a concrete shared object reference of the same type. You can customize a shared object by adding, deleting, or modifying an entry in the mapping table.

The regional server admin can customize polymorphic objects by adding local, concrete shared objects to it. The mapping table shows only the current domain’s entries. Therefore, if an admin is in the global domain, no subdomain entries are visible.

This section contains the following topics:

- Access Control of Polymorphic Object
- Validation of Polymorphic Object
- Supported Polymorphic Object Categories

Access Control of Polymorphic Object

The following table defines accessibility of polymorphic objects in different server.

Table 32: Polymorphic Objects

<table>
<thead>
<tr>
<th></th>
<th>Polymorphic objects created and used in Central Manager Server</th>
<th>Polymorphic objects created in a Central Manager, but used in a regional server</th>
<th>Polymorphic objects created and used in a regional server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Customize mapping table</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Change name/color and other attributes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Delete</td>
<td>Yes</td>
<td>Yes if not referenced by central rules.</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Validation of Polymorphic Object
When an admin first creates a polymorphic object, the customization state is set to pending. The validation routine generates a warning/error message when encountering the pending state. Validation of a polymorphic object is triggered if an object is used by a rule and that rule is edited or viewed in the policy manager.

Supported Polymorphic Object Categories
Polymorphic objects are in the same category as concrete objects of the same nature. The shared object type attribute includes a new value for polymorphic objects of a specific category. The following objects categories can have polymorphic type: Address, Service, Zone, and Global NAT.

Zone is a polymorphic shared object at the Central Manager level. After a global pre/post rule is pushed, zone objects resolve into names in pre/post rules. A vsys zone can only be supported with a polymorphic zone. Admins must map every vsys manually with a vsys zone name.

Global MIP/DIP/VIP objects in current NSM are intrinsically polymorphic. For all other categories of shared objects at Central Manager level, only concrete shared objects are supported.

Manage Polymorphic Objects
Polymorphic objects can be created in either at the Central Manager level or the regional server level. When polymorphic objects are created in the Central Manager they are pushed to one or more regional servers where they are available to be populated with real values.

The workflow for using polymorphic objects is:
- Create a Polymorphic Object
- Add a Polymorphic Object to a Pre/Post Rule
- Map a Polymorphic Object to a Real Value

Create a Polymorphic Object
This procedure assumes that a Central Manager admin is logged onto a Central Manager client.

To create a polymorphic object:
1. In the main navigation tree, select Object Manager.
2. Select one of the following objects that can be polymorphic objects.
   - Address
   - Service
   - Zone
3. Click the Add icon in the toolbar and select **Polymorphic Address** to open the **Add Polymorphic Address** dialog box.

4. Enter the following information for the new polymorphic address, then click **OK**.
   - Name
   - Color (optional)
   - Comment (optional)
NSM adds the polymorphic address object to the address tree.

Add a Polymorphic Object to a Pre/Post Rule

This procedure assumes that a Central Manager admin is logged onto a Central Manager client.

To create a polymorphic object:

1. In the main navigation tree, select **Policy Manager > Central Manager Policies**.
2. Select either **Central Manager Pre Rules** or **Central Manager Post Rules**.
3. Click the Add icon in the toolbar and select **Polymorphic Address**.
Polymorphic objects have a color-coding of green and are ready to be used by Central Manager pre/post rules.

4. Drag the polymorphic object from the **Shared Objects** section to the **Destination** column in Figure 114.

Map a Polymorphic Object to a Real Value

The following procedure assumes that a Central Manager admin is logged onto a Central Manager client and a regional server object has been created.

To map a polymorphic object to a real value:

1. In the toolbar, click the **Login to Regional Server** drop down list.
2. Select one or more of the available regional servers and click **OK**. If you are prompted to save any changes, select the appropriate option.

The Job Manager provides a status window for pushing the polymorphic object to the selected regional server(s).

3. In the main navigation tree of the regional server, select **Object Manager > Address Object** to show the polymorphic address objects pushed to this regional server.

4. Double-click the object you want to map to a real value.

Figure 116: Polymorphic Address Object in a Regional Server

5. Click the Add icon in the toolbar to open the **New Address Map Entry** dialog box.

Figure 117: Add an Address Map Entry
6. Enter the values of the address object you want to map and click **OK** to map real values to the polymorphic object you pushed to the regional server.

Figure 118: Apply Values to Polymorphic Object
Chapter 10
Configuring VPNs

VPNs route private data through a public Internet. Like normal Internet traffic, data in a VPN is routed from source to destination using public Internet networking equipment. Unlike normal traffic, however, the source and destination use a Security Association (SA) pair to create a secure, private tunnel through which the data traverses the Internet. A tunnel has a defined start point and end point, (usually an IP address), and is a private connection through which the data can move freely. By encrypting and authenticating the data while in the tunnel, you can ensure the security and integrity of the data.

VPNs can also connect widely distributed networks to make separate networks appear as a single Wide Area Network (WAN). VPNs replace costly point-to-point protocol (PPP) and frame relay connections that require dedicated lines (and sometimes even satellites!) between your private networks.

This chapter contains the following sections:

- About VPNs on page 416
- Planning for Your VPN on page 417
- Preparing VPN Components on page 427
- Creating VPNs with VPN Manager on page 434
- VPN Manager Examples on page 452
- Creating Device-Level VPNs on page 474
- Device-Level VPN Examples on page 489

This chapter discusses the concepts involved in creating secure tunnels between devices, details the differences between VPN types, helps you determine the best VPN for your network, and guides you through creating and configuring your chosen VPN.

NOTE: For step-by-step instructions on creating VPNs, see the NetScreen-Security Manager Online Help Topic “VPNs”.

415
About VPNs

With Juniper Networks NetScreen-Security Manager, you can use basic networking principles and your Juniper Networks security devices to create VPNs that connect your headquarters with your branch offices and your remote users with your protected networks.

NetScreen-Security Manager supports tunnel and transport modes for AutoKey IKE, Manual Key, L2TP, and L2TP-over-AutoKey IKE VPNS in policy or route-based configurations. You can create the VPN at the system-level or device-level:

- **System-Level VPN (VPN Manager)**—Design a system level VPN and automatically set up connections, tunnels, and rules for all devices in the VPN.
- **Device-Level VPN (Device Manager)**—Manually configure VPN information for each security device, then add VPN rules to a Security Policy to create a policy-based VPN or configure routes on each security device to create a route-based VPNs.

---

**NOTE:** Each VPN that a device belongs to reduces the maximum number of templates by one. This includes VPNs configured in VPN Manager and VPNs configured at the device-level. You can apply a maximum of 63 templates to a single device.

---

**Creating System-Level VPNs with VPN Manager**

For AutoKey IKE and L2TP VPNs, create the VPN at the system-level using VPN Manager. VPN Manager supports:

- **AutoKey IKE VPNs**—In policy-based or route-based modes. You can also create a Mixed-Mode VPN to connect policy-based VPN members to route-based VPNs members in a single VPN.

- **L2TP-over-AutoKey IKE RAS VPNs and L2TP RAS VPNs**—Can connect and authenticate multiple L2TP remote access services (RAS) users and protected resources with or without encryption.

- **Re-usable VPN Components**—Create objects to represent your protected resources, CA certificates and CRLs, custom IKE proposals, and NAT configurations, then use these objects in multiple VPNs.

- **Compact and Expanded Views**—Choose the Compact (default) or Expanded view to create your VPN. Both views offer the same configuration options.

- **Autogenerated Tunnels**—Create tunnel interfaces on each route-based VPNs member automatically. Use the device tunnel summary to review all autogenerated tunnels in the VPN.

- **Autogenerated VPN Rules**—Create all VPN rules with a single click. NetScreen-Security Manager automatically generates the rules between each policy-based VPN member. You can review these rules, configure additional rule options (such as traffic shaping, attack protection, and logging), then insert the rules into a Security Policy.
Autogenerated VPN Routes—Automatically add virtual router information using the VPN Manager for each device based on the routing type. Specify a routing type of topology to autogenerate a route for all VPN members based on the configured routing type (static or dynamic). This information changes the tunnel interface data and virtual router data for each device.

To view all VPNs created with VPN Manager, select VPN Manager in the navigation tree. A list of saved VPNs appears in the main display area in table format. You can add and delete VPNs from this view.

VPN Manager does not support Manual Key VPNs; to create a Manual Key VPN in NetScreen-Security Manager, you must create the VPN at the device-level in Device Manager.

Creating Device-Level VPNs in Device Manager
For Manual Key VPNs, create the VPN at the device-level by manually configuring VPN information for each security device.

After you have configured the VPN on each security device in the VPN, add VPN rules to a Security Policy to create the VPN tunnel (for policy-based VPNs) or to control traffic through the tunnel (for route-based VPNs).

You can also create AutoKey IKE, L2TP, and L2TP-over-AutoKey IKE VPNs at the device-level.

Supported VPN Configurations
NetScreen-Security Manager supports all possible VPN configurations that are supported by the CLI and Juniper Networks ScreenOS WebUI, including:

- NAT-Traversal—Because NAT obscures the IP address in some IPSec packet headers, VPN nodes cannot receive VPN traffic that passes through an external NAT device. To enable VPN traffic to traverse a NAT device, you can use NAT Traversal (NAT-T) to encapsulate the VPN packets in UDP. If a VPN node with NAT-T enabled detects an external NAT device, it checks every VPN packet to determine if NAT-T is necessary.

- XAuth—To authenticate remote access services (RAS) users, use XAuth to assign users an authentication token (such as SecureID) and to make TCP/IP settings (IP address, DNS server, and WINS server) for the peer gateway.

Planning for Your VPN
NetScreen-Security Manager offers you maximum flexibility for creating a VPN. You can choose your topology, authentication level, and creation method. Because you have so many choices, it’s a good idea to determine what your needs are before you create the VPN so you can make the right decisions for your network.

These decisions include:

- VPN Topology—What do you want to connect? How many devices? How do you want these devices to communicate? Will you have users as VPN members?
Data Protection—How much security do you need? Do you need encryption, authentication, or both? Is security more or less important than performance?

Tunnel Type—Do you want an always-on connection or traffic-based connection?

VPN Manager or Device-Level—How do you want to create the VPN? Maintain the VPN?

The following sections provide information to help you make these decisions.

**Determining Your VPN Members and Topology**

You can use a VPN to connect:

- Security devices—Create a VPN between two or more security devices to establish secure communication between separate networks.
- Network components—Create a VPN between two or more network components to establish secure communication between specific machines.
- Remote users—Create a VPN between a user and a security device to enable secure access to protected networks.

---

**NOTE:** In NetScreen-Security Manager, remote users are known as remote access service (RAS) users.

Each device, component, and RAS user in a VPN is considered a VPN node. The VPN connects each node to other nodes using a VPN tunnel. VPN tunnel termination points are the end points of the tunnel; traffic enters and departs the VPN tunnel through these end points. Each tunnel has two termination points: a source and destination, which are the source and destination zones on security device.

**Using Network Address Translation (NAT)**

Network Address Translation (NAT) maps private IP addresses to public, Internet-routeable IP addresses. Because your security device is also a NAT server, you can use private, unregistered IP addresses for your internal network, minimizing the number of registered IP addresses you must buy and use.

If you enable NAT, when an internal system connects to the Internet, the security device translates the unregistered IP address in the outbound data packets to the registered address of the security device. The security device also relays responses back to the original system. Additionally, because your internal systems do not have a valid Internet IP address, your systems are invisible to the outside Internet, meaning that attackers cannot discover the IP addresses in use on your network.

**Site-to-Site**

Site-to-site VPNs are the most common type of VPN. Typically, each remote site is an individual security device or RAS user that connects to a central security device.

- **Advantages**—Simple, easy to configure.
Disadvantages—The central security device is a single point of failure.

Use a site-to-site VPN to connect remote networks to a single, central network inexpensively. An example is shown below:

Figure 119: Site-to-Site VPN Overview

Hub and Spoke

In a hub and spoke VPN, multiple security devices (spokes) communicate through a central device (the hub).

Advantages—Can connect several devices and users. Hub and spoke VPNs are easy to maintain because you only need to reconfigure the spoke and the hub device, which save you administration and resource costs. If you have smaller security devices with limited tunnel capacity, you can use hub and spoke VPNs to increase the number of available tunnels.

Disadvantages—The hub is a single point of failure; however, you can use NSRP for redundancy.

A hub acts as a concentrator for the other VPN members, but does not necessarily have resources that are available to other members. In fact, you can specify a security device that is not a VPN member to act as the hub: If you include the hub in the VPN, the hub device can send and receive traffic from all spokes; if you do not include the hub, the hub device 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:

Figure 121: Full Mesh VPN Overview
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.

Protecting Data in the VPN
To protect traffic as it passes over the Internet, you can create a secure tunnel between devices using a tunneling protocol. Each device in the VPN uses the tunneling protocol to establish a secure data path, enabling traffic between the devices to flow securely from source to destination. NetScreen-Security Manager provides two tunneling protocols, IPSec and L2TP, as detailed in the following sections.

Using IPSec
IPSec is a suite of related protocols that tunnel data between devices and cryptographically secure communications at the network layer. Each device in the VPN has the same IPSec configuration, enabling traffic between the devices to flow securely from source to destination.

Because IPSec functions at the network layer, it protects all data generated by any application or protocol that uses IP. Network layer encryption protects data generated by all protocols at the upper layers of the protocol stack. It also protects all data throughout the entire journey of the packet. Data is encrypted at the source and remains encrypted until reaching its destination. Intermediate systems that transmit the packet (like routers and switches on the Internet) do not need to decrypt the packet to route it, and do not need to support IPSec.

When you create your VPN in NetScreen-Security Manager, you can use one or more IPSec services to establish the tunnel and protect your data. Typically, VPNs use encryption and authentication services to enable basic security between devices; however, for critical data paths, using certificates can greatly enhance the security of the VPN. NetScreen-Security Manager supports the following IPSec data protection services for VPNs.

Using Authentication
To authenticate the data in the VPN tunnel, you can use the AH protocol, pre-shared secrets, or certificates:

- **Authentication Header (AH)**—AH authenticates the integrity and authenticity of data in the VPN. You can authenticate packets using Message Digest version 5 (MD5), Secure Hash Algorithm-1 (SHA-1), or Hash-based Message Authentication Code (HMAC).

- **Preshared Secret**—NetScreen-Security Manager generates an ephemeral secret, distributes the secret to each VPN node, then authenticates the VPN data using MD5 or SHA hash algorithms against the secret.

- **Certificates**—IKE uses a trusted authority on the client as the certificate server. For details on using certificates, see “NetScreen-Security Manager: Configuring Firewall/VPN 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.

**Using Encapsulating Security Payload (ESP)**

ESP encrypts the data in the VPN with DES, Triple DES, or AES symmetric encryption. When the encrypted data arrives at the destination, the receiving device uses a key to decrypt the data. For additional security, you can encrypt the keys that decrypt the data using Diffie-Hellman asymmetric encryption. ESP can also authenticate data in the VPN using MD5 and SHA-1 algorithms. You can use ESP to encrypt, authenticate, or encrypt and authenticate data depending on your security requirements.

**NOTE:** We strongly recommend that you do not use null AH with ESP.

Because ESP uses keys to encrypt and decrypt data, each VPN node must have the correct key to send and receive VPN data through the VPN tunnel.

You can manually configure a key for each VPN node, or use a key exchange protocol to automate key generation and distribution:

- **Manual Key IKE**—In a manual key VPN, you specify the encryption algorithm, authentication algorithm, and the Security Parameter Index (SPI) for each VPN node. Because all security parameters are static and consistent, VPN nodes can send and receive data automatically, without negotiation.

- **Autokey IKE**—In an AutoKey IKE VPN, you can use the Internet Key Exchange (IKE) protocol to generate and distribute encryption keys and authentication algorithms to all VPN nodes. IKE automatically generates new encryption keys for the traffic on the network, and automatically replaces those keys when they expire. Because IKE generates keys automatically, you can give each key a short life span, making it expire before it can be broken. By also exchanging authentication algorithms, IKE can confirm that the communication in the VPN tunnel is secure.

Because all security parameters are dynamically assigned, VPN nodes must negotiate the exact set of security parameters that will be used to send and receive data to other VPN nodes. To enable negotiations, each VPN node contains a list of proposals; each proposal is a set of encryption keys and authentication algorithms. When a VPN node attempts to send data through the VPN tunnel, IKE compares the proposals from each VPN node and selects a proposal that is common to both nodes. If IKE cannot find a proposal that exists on both nodes, the connection is not established.

IKE negotiations include two phases:

- In Phase 1, two members establish a secure and authenticated communication channel.

- In Phase 2, two members negotiate Security Associations for services (such as IPsec) that require key material and/or parameters.

VPN nodes must use the same authentication and encryption algorithms to establish communication.
Replay protection—In a replay attack, an attacker intercepts a series of legitimate packets and uses them to create a denial-of-service (DoS) against the packet destination or to gain entry to trusted networks. Replay protection enables your security devices to inspect every IP packet to see if the packet has been received before—if packets arrive outside a specified sequence range, the security device rejects them.

Using L2TP

Layer 2 Tunneling Protocol (L2TP) is another tunneling protocol used to transmit data securely across the Internet. Because L2TP can transport Point to Point Protocol (PPP) frames over IP, it is often used to:

- Establish PPP connections (Ex. authenticate ADSL services using PPP for users with an ISP at the opposite side of a Telco IP/ATM network)
- Transmit non-IP protocols (Ex. bridge Novell and other network protocols)

PPP can send IP datagrams over a serial link, and is often used to enable dial-up users to connect to their ISP and to the Internet. PPP authenticates username and password, and assigns parameters such as IP address, IP gateway, and DNS. PPP can also tunnel non-IP traffic across a serial link, such as Novell IPX or AppleTalk.

PPP is also useful because it can carry non-IP traffic and authenticate connections to RADIUS servers. However, because PPP is not an IP protocol, Internet routers and switches cannot route PPP packets. To route PPP packets, you use L2TP, which encapsulates PPP packet inside an Internet routeable, UDP packet. L2TP VPNs supports remote access service users using Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP) authentication.

Using L2TP Over AutoKey IKE

L2TP only transmits packets; for encryption, authentication, or other data protection services, you must further encapsulate the L2TP packet using AutoKey IKE.

Choosing a VPN Tunnel Type

You can configure three types of VPN tunnels with NetScreen-Security Manager:

- Policy-based VPNs—The VPN tunnel is created and maintained only during the transfer of network traffic that matches a VPN rule, and is torn down when the connection ends. Use policy-based VPNs when you want to encrypt and authenticate certain types of traffic between two VPN members.

- Route-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 Policy-based and Route-based VPN types.
About Policy-Based VPNs

A policy-based VPN tunnels traffic between two security devices or between one security device and a remote user. Each time a security device detects traffic that matches the from zone, source, to zone, destination, and service in the VPN rule, it creates the VPN tunnel to encrypt, authenticate, and send the data to the specified destination. When no traffic matches the VPN rule, the firewall tears down the VPN tunnel.

To create a policy-based VPN, use NetScreen-Security Manager to configure a policy based on the network components you want to protect, including protected resources, then push the configuration to the security device(s). The security device(s) use the configuration to create the VPN tunnel. A protected resource is a combination of a network component and a service; protected resources in a VPN can communicate with other protected resources using the specified services. In a VPN rule, you add protected resources as the source and destination IP addresses.

Policy-based VPNs can use any of the supported data protection methods. Use policy-based VPNs when you want to enable Remote Access Services (RAS). You can add users to the VPN just as you add devices, enabling user access to all resources within the VPN.

About Route-Based VPNs

Like a policy-based VPN, a route-based VPN tunnels traffic between two security devices or between one security device and a remote user. However, a route-based VPN automatically tunnels all traffic between two termination points, without regard for the type of traffic. Because the tunnel is an always-on connection between two network points, the security device views the tunnel as a static network resource through which to route traffic.

To create the termination points of the tunnel, you designate an interface on the security device as a tunnel interface, then define a static route or use a dynamic routing protocol (BGP, OSPF) between all tunnel interfaces in the VPN. The tunnel interface, just like a physical interface, maintains state to enable dynamic routing protocols to make route decisions. When using VPN Manager to create your route-based VPNs, the tunnel interfaces are automatically created for you.

VPN Checklist

After you have carefully considered your VPN requirements, create a VPN checklist to help you determine the VPN components you need to create. You might also want to create a network diagram of your topology that includes protected resources, VPN members, their IP addresses and gateways, and the type of tunnel between them.

Define Members and Topology
What do you want to connect?

- Devices
- Network Components/Protected Resources
- Remote Access Service (RAS) Users
Extranet Devices

How do you want to connect the VPN members?

- Site to Site
- Hub and Spoke
- Full Mesh

You might want to create a network diagram to map out your VPN visually, with IP addresses, to help you configure your topology.

Define VPN Type: Policy-Based, Route-Based, or Mixed-Mode

What type of traffic do you want to protect?

- Use a policy-based VPN to encrypt and authenticate certain types of traffic between two network nodes.
- Use a route-based VPNs 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 VPNs nodes.

Define Security Protocol (Encryption and Authentication)

How do you want to protect the VPN traffic?

- Autokey IKE
- L2TP
- L2TP over AutoKey IKE
- Manual Key (you cannot use VPN Manager to create a Manual Key VPN)

You must also decide if you want to use certificates to authenticate communication between the VPN members.

Define Method: VPN Manager or Device-Level?

How do you want to create the tunnel? Using VPN Manager or configuring each device?

Using VPN Manager

When adding a VPN using the VPN Manager, you enter the VPN members, gateways, IKE properties, and VPN topology, then autogenerate the VPN rules that create the VPN. You can inspect the VPN rules and override any VPN property before sending the VPN configuration to your devices.

Choose the VPN type that best matches your VPN requirements:
- Autokey IKE VPN—Use to authenticate and encrypt traffic between devices and/or protected resources. An Autokey IKE VPN supports:
  - Mixed-mode VPNs (policy-based members and route-based members)
  - Policy-based VPNs
  - Route-based VPNs
  - ESP and AH Authentication
  - ESP AutoKey IKE Encryption
  - IP traffic
  - Tunnels between devices (routing-based) and protected resources (policy-based)

- Autokey IKE RAS VPN—Use to authenticate and encrypt traffic between remote users and protected resources. An Autokey IKE RAS VPN supports:
  - Policy-based VPNs
  - ESP and AH Authentication
  - ESP AutoKey IKE Encryption
  - IP traffic
  - Remote access users

- L2TP RAS VPN—Use to authenticate (but not encrypt) PPP or other non-IP traffic between RAS users and protected resources. An L2TP RAS VPN supports:
  - Policy-based VPNs
  - AH Authentication
  - PPP or other non-IP traffic
  - Remote access users

- L2TP over Autokey IKE RAS VPN—Use to authenticate and encrypt PPP traffic between remote users and protected resources. An L2TP over Autokey IKE RAS VPN supports:
  - Policy-based VPNs
  - ESP and AH Authentication
  - ESP AutoKey IKE Encryption
  - PPP or other non-IP traffic
  - Remote access users
Creating Device-Level VPNs

You can create the following VPN types:

- AutoKey IKE VPN
- Manual Key IKE VPN
- L2TP VPN
- Redundant Site-Site VPN

Preparing VPN Components

After you have determine how you want to configure your VPN, you can begin preparing the VPN components necessary to create the VPN. A VPN combines device-level components (such as devices, zones, and routes) with network-level components (authentication, users, and NAT) to create a secure system of communication. Before you can create a VPN, you must first configure the components that comprise the VPN.

Each VPN type has basic, required, and optional components:

- Preparing Basic VPN Components
- Preparing Required Policy-Based VPN Components
- Configuring Required Routing-Based VPN Components
- Configuring Optional VPN Components

For mixed-mode VPNs, you must configure all basic and required policy- and route-based components.

NOTE: For step-by-step instructions on creating VPNs, see the NetScreen-Security Manager Online Help topic “VPNs”.

Preparing Basic VPN Components

To create any type of VPN, ensure that all security devices you want to use in the VPN are managed by NetScreen-Security Manager and configured correctly.

- Devices—Add the security devices you want to include in the VPN to NetScreen-Security Manager, ensuring that all devices are in the same domain. If you need to add a device to a VPN in a different domain, you must add the device as an extranet device in the domain that contains the VPN, then add the extranet device to the VPN. For details on adding devices, importing devices, or using extranet devices in VPNs, see “Domain selection is critical when using VPNs. You can create VPNs only between devices within the same domain. If you need to add a device to a VPN in a different domain, add the device as an extranet device in the domain that contains the VPN, then add the extranet device to the VPN (as shown in Figure 24).” on page 84.
Zones—Configure each security device with at least two zones (trust and untrust); each zone must contain at least one interface (physical or virtual). For details on creating and configuring zones and interfaces, see Chapter 5, “Configuring Devices”.

### Preparing Required Policy-Based VPN Components

A policy-based VPN requires several components:

- **Address Objects**
- **Protected Resources**
- **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 “Configuring Address Objects” on page 227.

### Configuring Protected Resources

You should determine your protected resources first to help you identify the devices you need to include in the VPN. After you know what you want to protect, you can use VPN Manager or manually configure your security devices to create the VPN. A protected resource object represents the network components (address objects) and services (service objects) you want to protect and the security device that protects them.

The address specifies secured destination, the service specifies the type of traffic to be tunneled, and the device specifies where the VPN terminates (typically an outgoing interface in untrust zone). In a VPN rule, protected resources are the source and destination IP addresses.

When creating protected resources:

- To protect multiple network components that are accessible by the same security device, add the address objects that represent those network components to the protected resource object.

- To protect a single network component that is accessible by multiple security devices, add multiple devices to the protected resource object. You must configure each device to be a part of the VPN.

- To manage different services for the same network component, create multiple protected resource objects that use the same address object and security device but specify a different service object.
If you change the security device that protects a resource, NetScreen-Security Manager removes the previous security device from all affected VPNs and adds the new security device. However, NetScreen-Security Manager does not configure the VPN topology for the new security device—you must reconfigure the topology to include the new device manually.

For more details on creating protected resources, see “Configuring Protected Resources” on page 313.

Configuring Shared NAT Objects

For VPNs that support policy-based NAT, you must create one or more shared NAT objects. A shared NAT object contains references to device-specific NAT objects, enabling multiple devices to share a single object.

First, create a device-specific NAT object by editing the device configuration of each security device member. Then, create a global NAT object that includes the device-specific NAT objects. In the Object Manager, create a single shared NAT object to represent similar device-specific NAT objects (for example, a global DIP represents multiple device-specific DIPs). Use the global NAT object in your VPN; when you install the VPN on a device, that device automatically replaces the shared NAT object with its device-specific NAT object.

For details on shared NAT objects, see “Configuring NAT Objects” on page 308.

Configuring Remote Access Service (RAS) Users

For VPNs that support RAS users, you must create a User Object to represent each user. NetScreen-Security Manager supports two types of users:

- Local Users—A local user has an account on the security device that guards the protected resources in the VPN. When a local user attempts to connect to a protected resource, the security device authenticates the user.

- External Users—An external user has an account on RADIUS or SecureID Authentication Server. When an external user attempts to connect to a protected resource, the security device forwards the request to the authentication server for authentication.

Authenticating RAS Users

You can authenticate/encrypt a RAS user using one or more of the following protocols:

- XAuth—Uses IPSec ESP and a username and password for authentication. XAuth RAS users must authenticate with a username and password when they connect to the VPN tunnel.
- **AutoKey IKE**—Uses IPSec ESP and AH for encryption and authentication. AutoKey IKE users have a unique IKE ID that NetScreen-Security Manager uses to identify and authenticate the user during IKE Phase I negotiations. To simplify RAS management for large numbers of AutoKey IKE users, you can also create AutoKey IKE groups that use a shared Group IKE ID.

**NOTE:** We strongly recommend that you do not use null AH with ESP.

- **L2TP**—Uses Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP) for authentication (password sent in the clear).

- **Manual Key IKE**—Uses IPSec ESP and AH for encryption and authentication. Because manual key users are device-specific, you create them in the security device configuration, not in the Object Manager. For details on creating manual key users, see “NetScreen-Security Manager: Configuring Firewall/VPN Devices”.

NetScreen-Security Manager allows certificate with DC in certificate DN to be used for dialup user IKE ID selection.

When you use certificate DN as dialup user IKE ID, the following takes place:

- On the device sever, a partial or whole DN is associated with a VPN configuration.

- On the client side, the certificate DN is sent as IKE ID for the server to match the VPN configuration based on the content of DN.

The server DN configuration can contain a container part and a wildcard part as follows:

- The container part contains a continuous section of the DN, eg. “OU=a,O=b”. Any DN containing all specified elements in correct order are accepted.

- Up to seven wildcards can be specified, one for each of the following element: CN, OU, O, L, ST, C, Email.

NetScreen-Security Manager needs to support DC container type when using ASN1-DN to create IKE ID or a group of IKE ID that enables multiple, concurrent connections to the same VPN tunnel. During Phase 1 negotiations, IKE first attempts to make an exact match between the RAS IKE ID and peer gateway IKE ID.

If no match is found, IKE then attempts to make a partial match between the RAS IKE ID and Group IKE ID. When selecting this type, you must enter a container identity or a wildcard ID (CN, OU, O, L, ST, C, Email).

NetScreen-Security Manager devices authenticate a RAS IKE user’s ID if the values in the RAS IKE user’s ASN-1DN identity fields exactly match the values in the group IKE user’s ASN1-DN identity fields. The container ID type supports multiple entries for each identity field (for example, “ou= eng,ou= sw,ou= screenos”). The ordering of the values in the identity fields of the two ASN1-DN strings must be identical. In this IKE ID matching part, we need to allow DC element to be matched.
NetScreen-Security Manager also supports DC in wildcard when using ASN1-DN to create IKE ID or a group of Wildcard ID.

NetScreen-Security Manager devices authenticate a RAS IKE user's ID if the values in the RAS IKE user's ASN1-DN identity fields match those in the group IKE user's ASN1-DN identity fields. The wildcard ID supports only one value per identity field (for example, "ou= eng" or "ou= sw", but not "ou= eng, ou= sw"). The ordering of the identity fields in the two ASN1-DN strings are inconsequential. In this IKE ID matching part, we need to support DC as a wildcard element.

Configuring Group IKE IDs
If your VPN includes multiple remote users, it can be impractical to create an IKE ID and VPN rule for each. Instead, you can use a Group IKE ID to authenticate multiple users in a single VPN rule. In the security device configuration VPN settings, create a VPN Group and specify the maximum number of concurrent connections that the group supports (cannot exceed the maximum number of allowed Phase 1 SAs or the maximum number of VPN tunnels allowed on the Juniper Networks security device platform).

For details on group IKE IDs, see the ScreenOS 5.x Concepts and Examples Guide.

Configuring Required Routing-Based VPN Components
A route-based VPNs requires two components:

- Tunnel Interface or Zone
- Route (Static or Dynamic)

The following sections detail how to configure each required component.

For VPNs created with VPN Manager, you create the VPN first to autogenerate the tunnel interfaces, then create the routes on the device itself using those tunnel interfaces. For VPNs created at the device level, you can create the tunnel interfaces and routes before or after configuring the VPN.

Configuring Tunnel Interfaces and Tunnel Zones
A VPN requires a physical or virtual interface on the security device, and each security device supports a specific number of physical and virtual interfaces. To support multiple VPNs on a device, you might want to create tunnel interfaces and tunnel zones to increase the number of available interfaces on the device.

**NOTE:** VPN Manager automatically creates the necessary tunnel interfaces for route-based VPNs. For device-level VPNs, you can create the tunnel interfaces before or after creating the VPN.

If you do not need to do address translation (NAT), use unnumbered.
Tunnel Interfaces—A tunnel interface handles VPN traffic between the VPN tunnel and the protected resources. You can create numbered tunnel interfaces that use unique IP addresses and netmasks, or unnumbered tunnel interfaces that do not have their own IP address and netmask (unnumbered tunnel interface borrows the IP address of the default interface of the security zone).

Tunnel Zones—A tunnel zone is a logical construction that includes one or more numbered tunnel interfaces. You must bind the VPN tunnel to the tunnel zone (not the numbered tunnel interfaces); the VPN tunnel uses the default interface for the tunnel zone. In a policy-based VPN, you can link:

- A single VPN tunnel to multiple tunnel interfaces
- Multiple VPN tunnels to a single tunnel interface

For details on tunnel interfaces and tunnel zones, see “NetScreen-Security Manager: Configuring Firewall/VPN Devices”.

Configuring Static and Dynamic Routes
A security device must know the path, or route, between each protected resource or security device in the VPN before it can forward packets from the source network to the destination network on the other side of the tunnel. To specify the route, you can use static routes, which define a specific, unchanging path between two VPN nodes, or dynamic routes, which define an algorithm that dynamically determines the best path between two VPN nodes.

NOTE: If you are using VPN Manager to create the route-based VPNs, you create the routes after autogenerating the VPN. If you are creating a device-level VPN, you can create the routes after configuring the tunnel interfaces.

To create a static route, you must manually create a route for each tunnel on each device. For VPNs with more than just a few devices, Juniper Networks highly recommends using a dynamic routing protocol to automatically determine the best route for VPN traffic:

To route between different networks over the Internet, use Border Gateway Protocol (BGP); to route within the same network, use Open Shortest Path First (OSPF). For details on creating routes, see “NetScreen-Security Manager: Configuring Firewall/VPN Devices”.

Configuring Optional VPN Components
In any type of VPN, you can also use three optional components:

- Authentication Server
- Certificate and Certificate Revocation List Objects
- PKI Defaults

The following sections detail how to configure each optional component; after you have created the component, you can use it to create your VPN.
Creating Authentication Servers

To externally authenticate VPN traffic for XAuth and L2TP, you must create an authentication server object to use in your VPN. For details on authentication servers, see “Configuring Authentication Servers” on page 289.

Creating Certificate Objects

To authenticate external devices, use a Group IKE ID to authenticate multiple RAS users, or provide additional authentication for the security devices in your VPN, you must obtain and install a digital certificate on each VPN member. A digital certificate is an electronic means for verifying identity through the word of a trusted third party, known as a Certificate Authority (CA). The CA is a trusted partner of the VPN member using the digital certificate as well as the member receiving it.

The CA also issues certificates, often with a set time limit. If you do not renew the certificate before the time limit is reached, the CA considers the certificate inactive. A VPN member attempting to use an expired certificate is immediately detected (and rejected) by the CA.

To use certificates in your VPN, you must configure:

- **Local Certificate**—Use a local certificate for each security device that is a VPN member.
- **Certificate Authority (CA) Object**—Use a CA object to obtain a local and CA certificate.
- **Certificate Revocation List (CRL) Object**—Use a CRL object to ensure that expired certificates are not accepted; a CRL is optional.

Configuring Local Certificates

A local certificate validates the identity of the security device in a VPN tunnel connection. To get a local certificate for a device, you must prompt the device to generate a certificate request (includes public/private key pair request) using the Generate Certificate Request directive. In response, the device provides certificate request that includes the encrypted public key for the device. Using this encrypted public key, you can contact an independent CA (or use your own internal CA, if available) to obtain a local device certificate file (a .cer file).

You must install this local certificate file on the managed device using NetScreen-Security Manager before you can use certificates to validate that device 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 “NetScreen-Security Manager: Configuring Firewall/VPN 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 NetScreen-Security Manager before you can use certificate to validate that device in your VPN. Because the CA certificate is an object, however, you can use the same CA for multiple devices, as long as those devices use local certificates that were issued by that CA.

You can also use SCEP to configure the device to automatically obtain a CA certificate at the same time it receives the local certificate. For details on configuring a certificate authority object, see “Configuring Certificate Authorities” on page 309.

Configuring CRL Objects
A Certificate Revocation List (CRL) identifies invalid certificates. You can obtain a CRL file (.crl) from the CA that issued the local certification and CA certificate for the device, then use this file to create a Certificate Revocation object.

You must install the CRL on the managed device using NetScreen-Security Manager before you can use a CRL to check for revoked certificates in your VPN. Because the CRL is an object, however, you can use the same CRL for multiple devices, as long as those devices use local and CA certificates that were issued by that CA.

After you have received a CRL list, you can use the CRL object in your VPN. For details on configuring a certificate revocation list object, see “Configuring CRL Objects” on page 312.

Creating PKI Defaults
You can configure default PKI settings for each security device that define how that device handles certificates. When configuring a VPN that includes the device, you can use these default settings. For details on PKI defaults, see “NetScreen-Security Manager: Configuring Firewall/VPN Devices”.

Creating VPNs with VPN Manager
Configuring a VPN using VPN Manager is an eight stage process:

- Adding the VPN
- Configuring Members (policy-based, RAS users, routing-based)
- Configuring Topology (AutoKey IKE only)
- Configuring Gateways
- Configuring IKE
- Autogenerating VPN Rules
- Configuring Overrides
- Adding the VPN Link

NOTE: For an L2TP RAS VPN, you do not need to configure gateways or IKE.
The following sections detail each step.

NOTE: For step-by-step instructions on creating VPNs, see the NetScreen-Security Manager Online Help topic “VPNs”.

Adding the VPN

From the menu bar, click VPN Manager > New and select the VPN type:

- **AutoKey IKE VPN**—Use to connect devices and/or protected resources. An AutoKey IKE VPN supports mixed-mode, policy-based, and routing-based VPNs, but does not support RAS users.

- **AutoKey IKE RAS VPN**—Use to connect IKE RAS users and protected resources. An Autokey IKE RAS VPN supports policy-based VPNs and IKE RAS users, but does not support routing-based VPNs, mixed-mode VPNs, or L2TP RAS users.

- **L2TP RAS VPN**—Use to connect L2TP RAS users and protected resources without encryption.

- **L2TP over AutoKey IKE RAS VPN**—Use to connect L2TP RAS users and protected resources. An L2TP over AutoKey IKE RAS VPN supports policy-based VPNs and L2TP RAS users, but does not support routing-based or mixed-mode VPNs.

Enter a name for the VPN, then specify the general properties for the VPN:

- **Enable**—Use this option to enable/disable the VPN. If you disable the VPN, the autogenerated VPN rules, VPN member gateways, and other device configuration settings are not installed on your managed devices.

- **Termination Point**—Select the Default Zone for the VPN Termination Point. Typically, the default zone is untrust. When you configure the topology for the VPN, you can select a unique termination point for each VPN member.

- **View Properties**—Configure the VPN components that the VPN Manager displays for the VPN:

  - **Type (AutoKey IKE VPN Only)**. Select the components you want to configure for the VPN: Route-based components, Policy-based components, or both. By default, VPN Manager displays all Route- and Policy-based components for an AutoKey IKE VPN.

  - **Dial Backup**. When enabled, VPN Manager displays the dial backup option for route-based components (dial backup is supported only on NetScreen-5GT devices running ScreenOS 5.1 and higher).

Click OK to save the VPN and return to VPN Manager.

Configuring Members

The second step in configuring your VPN is to add members to the VPN. Depending on the type of VPN you are creating, you can add protected resources, security devices, and/or RAS users as VPN members.
Adding Policy-Based Members

In policy-based configuration area, you can add protected resources to the VPN. Click Protected Resources link and select the predefined Protected Resources you want to include in the VPN. For details on creating Protected Resources, see “Configuring Protected Resources” on page 313.

After you have added the protected resources, you can configure NAT and/or L2TP settings on the security device that protects each resource:

- For L2TP RAS VPNs and L2TP over AutoKey IKE VPN protected resources, you must configure L2TP settings.
- For all protected resources, you can configure policy-based NAT. Use policy-based NAT to translate private source IP addresses to Internet-routeable IP addresses. Configuring NAT is optional; if you do not use NAT on your network, you do not need to configure NAT for the VPN.

The following sections detail how to configure NAT and L2TP.

Configuring NAT

Below the Protected Resources window, select NAT to display the protecting security devices for each protected resource. Select the device for which you want to configure NAT. Enable NAT and specify the following values (you cannot edit the name of the device or the zone that contains the protected resource).

- Configure Incoming DIP—You can enable the security device to use a Dynamic IP pool for incoming VPN traffic. For each incoming VPN packet, the device translates the destination address into a IP address that is selected from the DIP pool.
  - Interface for Incoming DIP. Select the interface that receives traffic addressed to Dynamic IP addresses.
  - Incoming Global DIP. Select the Global DIP object that represents range of IP addresses available to the security device. (This DIP pool must include IP addresses that are routeable on your internal network.)

For details on configuring DIP objects, see “Configuring DIP Objects” on page 308.

- Configure Tunnel Interface and Zone—You can bind the VPN tunnel to a tunnel interface or tunnel zone to increase the number of available interfaces in the security device.

NOTE: If the security device is running ScreenOS 5.x and configured in transparent mode, you can only configure the zone (the interface does not appear) ScreenOS 4.0.x devices display both zone and interface.

To use a tunnel interface and/or tunnel zone in your VPN, you must first create the tunnel interface or zone on the device; for details, see “Configuring Tunnel Interfaces and Tunnel Zones” on page 431 and “NetScreen-Security Manager: Configuring Firewall/VPN Devices”.
Tunnel Zone. Select a pre-configured tunnel zone on the security devices to bind the VPN tunnel directly to the tunnel zone. The tunnel zone must include one or more numbered tunnel interfaces; when the security devices route VPN traffic to the tunnel zone, the traffic uses one or more of the tunnel interfaces to reach the protected resources.

Tunnel Interface. Select a pre-configured tunnel interface on the security devices to bind the VPN tunnel to the tunnel interface. The security devices route all VPN traffic through the tunnel interface to the protected resources.

Configure MIP, VIP, and Outgoing DIP

- Enable MIP. Enable MIP to use a mapped IP address for the interface.
- Global MIP. Select the global MIP object that represents the mapped IP address you want to use for the interface.
- Global VIP. Select the global VIP object that represents the virtual IP address you want to use for the interface.
- Global DIP (Outgoing). You can enable the security device to use a Dynamic IP pool for outgoing VPN traffic. For each outgoing VPN packet, the device translates the source address into a IP address selected from the DIP pool. Select the Global DIP object that represents range of IP addresses available to the security device. (This DIP pool must include IP address that are routeable on the Internet.)

Configuring L2TP

For L2TP RAS VPNs and L2TP over AutoKey IKE VPN protected resources, you must configure L2TP settings.

To connect to an L2TP VPN tunnel, the L2TP RAS user uses the IP address and WINS/DNS information assigned by the user's ISP. However, when the L2TP RAS user sends VPN traffic through the tunnel, the security device assigns a new IP address and WINS/DNS information that enables the traffic to reach the destination network.

Below the Protected Resources pane, select L2TP/NAT to display the protecting security devices for each protected resource. (If you are configuring an AutoKey IKE VPN or AutoKey IKE RAS VPN, this option does not appear.) Select the device for which you want to configure L2TP. In the L2TP tab, specify the following values (you cannot edit the name of the device).

- Host Name—Enter the name of the L2TP host.
- Keep Alive—The number of seconds a VPN member waits between sending hello packets to an L2TP RAS user.
- Peer IP—Enter the IP address of the L2TP peer.
- Secret—Enter the shared secret that authenticates communication in the L2TP tunnel.
Remote Settings—Select the remote settings object that represents the DNS and WINS servers assigned to L2TP RAS users after they have connected to the tunnel.

IP Pool Name—Select the IP pool object that represents the available IP addresses that can be assigned to L2TP RAS users after they have connected to the tunnel.

Auth Server—Because the L2TP must authenticate L2TP users, use custom settings to associate those users with a specific Authentication Server. You can also configure the device to query the remote settings object for DNS and WINS information for those users.

To use the default authentication server for L2TP users, add the users to the device first.

NOTE: When configuring a VPN that includes RAS users, if you added the user as a L2TP local user and assigned an IP pool and remote settings object on a specific device in the VPN, those settings override the settings defined in the VPN.

Adding RAS Users
In the Remote User area, you can add RAS users to the VPN. (When configuring an AutoKey IKE VPN, this area does not appear.) Click the Users link to display the user selection dialog box, then click the Edit icon to select the predefined RAS users or user groups you want to include in the VPN. For details on creating RAS users and groups, see “Configuring User Objects” on page 298.

Defining a Default Gateway
You can include a single RAS user in multiple VPNs. To specify this VPN as the default entry point for all RAS users listed in the VPN, enable Use as Default Gateway.

Adding Routing-Based Members
In the routing-based configuration area, you can add routing-based members to the VPN. (When configuring an AutoKey IKE RAS VPN, an L2TP RAS VPN, or an L2TP over AutoKey IKE RAS VPN, this area does not appear.) A routing-based VPN member is a security device that will route traffic (statically or dynamically) through a tunnel interface to one or more VPN members.

VPN Manager automatically creates the necessary tunnel interfaces for each route-based VPNs member. However, after VPN Manager autogenerates the VPN tunnels, you must configure static or dynamic routes on the security devices to route traffic through these tunnel interfaces. For details on creating routes, see “NetScreen-Security Manager: Configuring Firewall/VPN Devices”.

Click the security devices link to display the route-based member selection dialog box.

Configure Tunnel Interface Settings—Select a Primary Zone, Secondary Zone, and physical source interface for each security device. The selected zone passes VPN traffic through the selected interface on the security device.
The Zone settings apply to all route-based members selected in the members window.

If the Primary Zone is not defined or available on the security device, VPN traffic automatically uses the Secondary Zone.

The Physical Source Interface is the default physical interface on the device that transmits VPN traffic.

Configure Tunnel Options—ScreenOS 5.x devices support additional functionality for handling VPN tunnels:

To use a single tunnel interface on each device for VPN traffic, enable Generate Single Tunnel Interface for 5.x devices. When enabled, the security device uses the route table and the next-hop tunnel binding table to link a specific destination to one of a number of VPN tunnels bound to the same tunnel interface. By mapping the next-hop gateway IP address specified in the route table entry to a specific VPN tunnel in the NHTB table, the device can use one tunnel interface for all VPN traffic through the device. This option is enabled by default.

To create entries in the Next Hop Tunnel Binding (NHTB) table, enable Generate NHTB entries for 5.x devices. When this option is selected, VPN Manager autogenerates NHTB entries for each VPN tunnel. If you are using a single interface for all VPN traffic on the device but you do not select this option, you must manually add the NHTB routes in the NHTB table, or configure BGP to automatically create the entries for you. This option is disabled by default.

For details on working with the NHTB routing table, see the Juniper Networks ScreenOS 5.x Concepts and Examples Guide, Volume 7, “Advanced VPN Features”.

Select Dial Backup to enable NetScreen-5GT security devices to use the serial port as a backup termination point for the VPN tunnel. When this option is enabled, VPN Manager automatically generates the termination point for the serial interface during VPN creation (you do not need to select the serial interface manually when configuring Termination Points).

Configure Members—Click the Add icon to select the predefined security devices you want to include in the VPN. After you have added the device to the VPN, you can double-click the device and configure overrides for the default tunnel interface zone, the physical source interface. For ScreenOS 5.x devices, you can also enable/disable single tunnel interface and NHTB entries.

After VPN Manager generates the tunnel interfaces, you must configure static or dynamic routes on each VPN member to route traffic to other VPN members.

Configuring Topology

In the general configuration area, you can define the topology and/or termination points of the VPN:
The topology of the VPN determines how VPN members logically connect to each other. The topology is the communication path that VPN traffic must take to reach a VPN member.

The termination points of the VPN determine how VPN members physically connect to each other. A termination point is the interface on each VPN member that sends and receives VPN traffic to and from the VPN tunnel.

**NOTE:** If you change the security device that protects a resource, NetScreen-Security Manager removes the previous security device from all affected VPNs and adds the new security device. However, NetScreen-Security Manager does not configure the VPN topology for the new security device—you must reconfigure the topology to include the new device manually.

For AutoKey IKE VPNs, you must define the topology for the VPN. Each VPN member is a node that has specific connection capabilities, and the topology describes the logical connections between those nodes.

A node can be:

- **Hub**—A hub can connect to a branch or main.

- **Main**—A main can connect to a hub, branch, or another main. When configuring a VPN that uses multiple mains, you can select to mesh all mains (all mains can communicate with each other) or disable all main meshing.

- **Branch**—A branch can connect to a hub or a main. Branches can send and receive VPN traffic to and from a hub or a main device, but cannot communicate directly with other branches.

Additionally, you can use a supernet to reduce the number of rules required for the hub device in a policy-based VPN. A supernet is an Address Object Group containing the network Address Objects that represent the source and destination points of the VPN. Use a supernet when the hub device supports a small number of rules.

### Configuring Common VPN Topologies

You can use VPN Manager to configure the following common VPN topologies:

- **Hub and Spoke**—Select a device to act as the hub; this device connects VPN members and enables them to communicate. Next, select the VPN members to be the spokes. You are not required to use a VPN member as a hub:
  - If do not select a VPN member as the VPN hub, the hub routes VPN traffic from one branch to another.
  - If you do select a VPN member as the VPN hub, the hub routes VPN traffic from itself and all connected branches.

  Each spoke can send and receive VPN traffic to and from the hub, but cannot communicate directly with other spokes.

**NOTE:** You can select only one hub per VPN.
Main and Branch—Main and branch topologies combine the flexibility of hub and spoke with the redundancy of full mesh. Because you can select multiple mains, each branch has an alternate tunnel to use if one main fails. To create a main and branch:

- Select the devices to act at mains; these devices can communicate with all other VPN members.
- Select remaining devices as branches; these devices communicate with all mains.

Full Mesh—Select all VPN members to act as mains. All members can communicate with any other VPN member. Do not select a hub.

Site to Site—Select both VPN members as mains. Each member can communicate with the other VPN member. Do not select a hub.

Defining Termination Points
You must define the termination interface for each security device in the VPN. The Termination Points tab displays the default termination points for the VPN. A termination point is the interface on a security device that sends and receives VPN traffic to and from the VPN tunnel, and is typically in the Untrust zone. Each VPN member (the security devices included as routing-based members and/or as protected resources for policy-based members) has a default termination interface.

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.

NOTE: You do not need to select the serial interface on a NetScreen-5GT security device to enable dial backup for the VPN tunnel. If you have enabled Dial Backup for the device in the Route-Based Configuration area, VPN Manager automatically generates the termination point for the serial interface during VPN creation.
Aggressive mode—The IKE identity of each node is not protected. The initiating node sends two messages and the receiving node sends one (three messages total); all messages are sent in the clear, including the IKE identity exchange between the nodes. Because Aggressive mode is typically faster but less secure than Main mode, use Aggressive mode when speed is more important than security.

For RAS VPNs, you must use Aggressive mode; for VPNs that do not include RAS users, select the mode that meets your requirements.

Configuring Heartbeats
Use heartbeats to enable redundant gateways.

- Hello—Enter the number of seconds the security devices wait between sending hello pulses.
- Reconnect—Enter the maximum number of seconds the security devices wait for a reply to the hello pulse.
- Threshold—Enter the number of seconds that the security devices wait before attempting to reconnect.

Configuring NAT Traversal
Because NAT obscures the IP address in some IPSec packet headers, VPN nodes cannot receive VPN traffic that passes through an external NAT device. To enable VPN traffic to traverse a NAT device, you can use NAT Traversal (NAT-T) to encapsulate the VPN packets in UDP. If a VPN node with NAT-T enabled detects an external NAT device, it checks every VPN packet to determine if NAT-T is necessary.

Because checking every packet impacts VPN performance, you should only use NAT Traversal for remote users that must connect to the VPN over an external NAT device. You do not need to enable NAT-T for your internal security device nodes that use NAT; each VPN node knows the correct address translations for VPN traffic and does not need to encapsulate the traffic.

To use NAT-T, enable NAT-Traversal and specify:

- UDP Checksum—A 2-byte value (calculated from the UDP header, footer, and other UDP message fields) that verifies packet integrity. You must enable this option for NAT devices that require UDP checksum verification; however, most NAT devices (including security devices) do not require it.
- Keep alive Frequency—The number of seconds a VPN node waits between sending empty UDP packets through the NAT device. A NAT device keeps translated IP addresses active only during traffic flow, and invalidates unused IP addresses. To ensure that the VPN tunnel remains open, you can configure the VPN node to send empty "keep alive" packets through the NAT device.

Configuring XAuth
Use the XAuth protocol to authenticate RAS users with an authentication token (such as SecureID) and to make TCP/IP settings (IP address, DNS server, and WINS server) for the peer gateway.
Default Server—To use the default XAuthentication server for the device. To change or assign a default XAuthentication server, edit the VPN settings in the security device configuration.

XAuth Server—Use when the remote gateway is a security device that you want to assign TCP/IP settings.

- Auth Server Name. Select a pre-configured authentication server object. For details on creating an authentication server object, see “Configuring Authentication Servers” on page 289.
- Allowed Authentication Type. Select Generic or Challenge Handshake Authentication Protocol (CHAP) (password is sent in the clear) to authenticate the remote gateway.
- Query Remote Setting. Enable this option to query the remote settings object for DNS and WINS information.

NOTE: When configuring a VPN that includes RAS users, if you added the user as a L2TP or XAuth local user and assigned a remote settings object on a specific device in the VPN, those settings override the settings defined in the VPN.

XAuth Client—Use when the remote gateway is a RAS user that you want to authenticate.

- Allowed Authentication Type. Select Any or CHAP.
- User Name and Password. Enter the user name and password that the RAS user must provide for authentication.

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

Bypass Authentication to permit VPN traffic from VPN members to pass unauthenticated by the XAuth server.

Configuring Gateway Security

Determine the authentication mechanisms you want the VPN nodes to use for IKE Phase 1 negotiations. You can use a preshared key or certificates for authentication.

Preshared Key/Certificate

For Phase 1, select a Preshared Key Information or PKI Information:

- Preshared Key—Use if your VPN includes security devices and/or RAS users. VPN nodes use the preshared key during Phase 1 negotiations to authenticate each other; because each node knows the key in advance, negotiations use fewer messages and are quicker.
To generate a random key, enter a value for the seed, then click Generate Key. NetScreen-Security Manager uses the seed value to generate a random key, which is used to authenticate VPN members.

NOTE: Using a random key can generate a key in excess of 255 characters, which exceeds ScreenOS limits and might not be accepted by the security device during update. To reduce the key size, shorten the autogenerated key value by deleting characters.

To use a predefined value for the key, enter a value for the Preshared Key.

PKI—Use if your VPN includes extranet devices or you require the additional security provided by certificates (PKI uses certificates for VPN member authentication). For details on creating and managing certificates, see “Configuring Certificate Authorities” on page 309.

For Phase 1, select a proposal or proposal set. You can select from predefined or user-defined proposals:

- To use a predefined proposal set, select one of the following:
  - Basic (nopfs-esp-des-sha, nopfs-esp-des-md5)
  - Compatible (nopfs-esp-3des-sha, nopfs-esp-3des-md5, nopfs-esp-des-sha, nopfs-esp-des-md5)
  - Standard (gs-esp-3des-sha, gs-esp-aes128-sha)

NOTE: You cannot use a predefined proposal set with certificates—you must select a user-defined proposal or change the authentication method to Preshared Key.

To use a user-defined proposal, select a single proposal from the list of predefined and custom IKE Phase 1 Proposals. For details on custom IKE proposals, see “Configuring IKE Proposals” on page 316.

If your VPN includes only security devices, you can specify one predefined or custom proposal that NetScreen-Security Manager propagates to all nodes in the VPN. If your VPN includes extranet devices, you should use multiple proposals to increase security and ensure compatibility.

Preshared Secrets

You can use the same preshared secret for all nodes in the VPN, or create a unique preshared secret for communication from a specific node to another node.

Configuring IKE IDs

Every VPN node has a unique identification number, known as an IKE ID. During Phase 1 negotiations, the IKE protocol uses the IKE ID to authenticate the VPN member.
VPN Manager automatically creates the default IKE ID for you, based on the policy- or route-based members and RAS users, so you do not need to configure this option. However, if you do not want to use the default IKE ID, you can select a different IKE ID type and configure an IKE ID for each VPN gateway.

The IKE ID tab displays all security devices included as routing-based members and/or as protected resources for policy-based members. For each device, select the IKE ID type and enter the ID value:

- **ASN1-DN**—Abstract Syntax Notation, version 1 is a data representation format that is non-platform specific; Distinguished Name is the name of the computer. Use ASN1-DN to create a Group IKE ID that enables multiple, concurrent connections to the same VPN tunnel; use a Group IKE ID to make configuring and maintaining your VPN quicker and easier.

  For details on how Group IKE IDs work, see “Configuring Group IKE IDS” on page 431. For details on determining the ASN1-DN container and wildcard values for Group IKE IDs, see the Juniper Networks ScreenOS 5.x Concepts and Examples Guide.

- **FQDN**—Use a Fully Qualified Domain Name when the gateway is a dynamic IP address. FQDN is a name that identifies (qualifies) a computer to the DNS protocol using the computer name and the domain name; ex. server1.colorado.mycompany.com.

- **IP Address**—Use an IP address when the gateway has a static IP address.

- **U-FQDN**—Use a User Fully Qualified Domain Name when the gateway is a dynamic IP address, such as a RAS user. A U-FQDN is an email address. For example: user1@mycompany.com.

### Configuring IKE

To configure the IKE properties and Phase 2 Proposals for the VPN, click the IKE Parameters link. Because L2TP RAS VPNs do not support encryption, you do not need to configure IKE properties for L2TP RAS VPNs.

**IKE Properties**

Configure the IKE properties:

- **Idle Time to Disable SA**—Configure the number of minutes before a session that has no traffic automatically disables the SA.

- **Replay Protection**—In a replay attack, an attacker intercepts a series of legitimate packets and uses them to create a denial-of-service (DoS) against the packet destination or to gain entry to trusted networks. If replay protection is enabled, your security devices inspect every IPSec packet to see if the packet has been received before—if packets arrive outside a specified sequence range, the security device rejects them.

- **IPSec Mode**—Configure the mode:
• Use tunnel mode for IPSec. Before an IP packet enters the VPN tunnel, NetScreen-Security Manager encapsulates the packet in the payload of another IP packet and attaches a new IP header. This new IP packet can be authenticated, encrypted, or both.

• Use transport mode for L2TP-over-AutoKey IKE VPNs. NetScreen-Security Manager does not encapsulate the IP packet, meaning that the original IP header must remain in plaintext. However, the original IP packet can be authenticated, and the payload can be encrypted.

• Do not set Fragment Bit in the Outer Header—The Fragment Bit controls how the IP packet is fragmented when traveling across networks.

• Clear. Use this option to enable IP packets to be fragmented.

• Set. Use this option to ensure that IP packets are not fragmented.

• Copy. Select to use the same option as specified in the internal IP header of the original packet.

Monitor
You can enable VPN Monitor and configure the monitoring parameters for the device. Monitoring is off by default. To enable the VPN Monitor in Realtime Monitor to display statistics for the VPN tunnel, configure the following:

• VPN Monitor—When enabled, the security devices in the VPN send ICMP echo requests (pings) through the tunnel at specified intervals (configurable in seconds) to monitor network connectivity (each device uses the IP address of the local outgoing interface as the source address and the IP address of the remote gateway as the destination address). If the ping activity indicates that the VPN monitoring status has changed, the device triggers an SNMP trap; the VPN Monitor (in RealTime Monitor) tracks these SNMP statistics for VPN traffic in the tunnel and displays the tunnel status.

• Rekey—When enabled, the security devices in the VPN regenerate the IKE key after a failed VPN tunnel attempts to re-establish itself. When disabled, each device monitors the tunnel only when the VPN passes user-generated traffic (instead of using device-generated ICMP echo requests). Use the rekey option to:

  • Enable dynamic routing protocols to learn routes and transmit messages through the tunnel.

  • Automatically populate the next-hop tunnel binding table (NHTB table) and the route table when multiple VPN tunnels are bound to a single tunnel interface.

For details on VPN monitoring at the device level, see the Juniper Networks ScreenOS 5.x Concepts and Examples Guide. For details on VPN Monitor (in Realtime Monitor) in NetScreen-Security Manager, see “Monitoring VPNs” on page 545.
Configuring Security Level

For Phase 2 negotiations, select a proposal or proposal set. You can select from predefined or user-defined proposals:

- To use a predefined proposal set, select one of the following:
  - Basic (nopfs-esp-des-sha, nopfs-esp-des-md5)
  - Compatible (nopfs-esp-3des-sha, nopfs-esp-3des-md5, nopfs-esp-des-sha, nopfs-esp-des-md5)
  - Standard (gs-esp-3des-sha, gs-esp-aes128-sha)

- To use a user-defined proposal, select a single proposal from the list of predefined and custom IKE Phase 2 Proposals. For details on custom IKE proposals, see “Configuring IKE Proposals” on page 316.

If your VPN includes only security devices, you can specify one predefined or custom proposal that NetScreen-Security Manager propagates to all nodes in the VPN. If your VPN includes extranet devices, you should use multiple proposals to increase security and ensure compatibility.

Autogenerating VPN Rules

When you have completed configuring the policy- and route-based VPNs members, the topology (if necessary) and termination points, and the IKE (if necessary) and gateway parameters for the VPN, you are ready to autogenerate the VPN.

During autogeneration, NetScreen-Security Manager generates the VPN rules that control traffic between policy-based VPN members, and edits the device configuration (gateways, security parameters, and so on) of each VPN member to support the VPN.

Autogeneration does not:

- Insert the VPN rules into a Security Policy. After you have reviewed the VPN rules and made any necessary overrides, you must manual insert the VPN rules (known as a VPN link) into a Security Policy. For details, see “Adding the VPN Link” on page 450.

- Install the new VPN rules or edited device configurations on the managed devices in the VPN. After you have inserted the VPN link into a Security Policy, you can install that policy on your devices using the Updated directive.

- Create static or dynamic routes for route-based VPNs.

To autogenerate the VPN, click Save.

Configuring Overrides

The override area enables you configure individual settings for each VPN rules (for policy-based and mixed-mode VPNs) and each VPN member. Each change you make to the autogenerated rules or VPN member configuration is known as an override to the VPN settings.
You might need to override the VPN settings to:

- Configure additional security for specific tunnels.
- Configure additional authentication between specific VPN members.
- Configure unique monitoring or reporting options for specific VPN members or VPN tunnels.
- Configure unique IKE IDs for each VPN member.

Editing Policy Rules

For policy-based and mixed-mode VPNs, NetScreen-Security Manager automatically generates the VPN rules to control traffic between VPN members. To view these autogenerated rules, click the Policy Rules link in the Overrides area; the rules appear in a separate NetScreen-Security Manager window, using the same row and column format as in the Security Policies.

NOTE: Policy rules do not appear for route-based VPNs.

Changing Rule Position

The position of the rules indicates the order that they apply to traffic. To change the position of a rule, you can:

- Right-click the rule and select Move Rule Up or Move Rule Down, or
- Right-click the rule and select Change Rule Position. In the New Position dialog box, enter a new rule number for this rule. (The rule number is the first column in the policy table.)

Filtering Rules

You can also filter the VPN rules by zones using the Zone Filter in the upper right-hand corner of the VPN rule window. Select a zone in From Zone and/or the To Zone to order the rules as desired.

To save this rule order, click Apply.

Configuring Rule Options

You can configure rule options for each rule, including traffic shaping, logging, AntiVirus and Attack Objects, and protection actions. For details on configuring these options, see “Configuring Firewall Rule Options” on page 335.

Editing Device Configuration

For all VPNs, you can edit the device configuration for each VPN member. The device configuration displays the interfaces, gateways, and other VPN configuration information for each individual device.
Overriding Interfaces
For route-based and mixed-mode VPNs, this displays the tunnel interfaces and virtual routers configured on the VPN member. To override the general properties and dynamic routing protocols for each tunnel interface, right-click the tunnel interface and configure the settings.

NOTE: The changes you make to a Virtual Router in the Overrides area apply to the device configuration, not just the VPN configuration. When you change a VR setting in VPN manager, that change is saved and applied to the device when you save and apply the VPN. Similarly, when you change a VR setting for the device configuration in Device Manager, that change is reflected in the VPN configurations that includes the device.

For policy-based VPNs, no tunnel interfaces appear.

Overriding AutoKey IKE VPN Settings
For VPNs that use AutoKey IKE, this displays the VPN name, remote gateway, and IPSec Mode for each tunnel in the VPN. To override the general properties, security, binding/proxyID, and monitoring option for each VPN tunnel, right-click the VPN name and configure the settings as desired.

Overriding Gateways
For all VPNs, this displays the gateway name, gateway mode, IP address, and IKE phase I proposals for each VPN gateway. To override the general properties, security, and IKE ID/XAuth options for each gateway, right-click the gateway name and configure the settings as desired.

Overriding VPN Groups
For all VPNs, this displays VPN groups.

Overriding L2TP Settings
For L2TP VPNs, this displays L2TP information for each VPN member. To edit this information, right-click and configure the settings as desired.

Viewing the Device Tunnel Summary
For route-based and mixed-mode VPNs, you can view the VPN tunnels between each route-based member, including the source and peer devices, the tunnel interface, zone, and physical interface.

NOTE: The device tunnel summary does not appear for policy-based VPNs.

You cannot edit the device tunnels from this view; to make overrides to the VPN tunnels, edit the interface configuration for each device.
Adding the VPN Link

After you have reviewed the autogenerated information and made any desired overrides to the VPN, you must update your managed devices to activate the VPN. By default, the VPN you created in VPN manager is installed as the first rule in the Security Policy for each managed device. However, the Security Policy does not display the VPN.

You can manually add a VPN link to your Security Policy; a VPN link creates a link between the Security Policy and VPN (the link points to the VPN rules that exist in the VPN in VPN Manager). You might want to add a VPN link so you can reposition it elsewhere in the policy, or to make the VPN viewable in your policy.

To create a VPN link, in Security Policies, select an existing Security Policy (or create a new Security Policy), then right-click and select Add VPN link. Select the VPN name and click OK to add the link to the policy. By default, the link appears at the top of the policy, but you can move the VPN link anywhere in the policy, just as you would a firewall rule.

If you make changes to the VPN or create overrides, the VPN link automatically updates to reflect those edits.
Editing VPNs

To edit a VPN created with VPN Manager:

1. In the navigation tree, select VPNs. A table listing all configured VPNs appears in the main display area.

2. Right-click the VPN you want to edit and select Edit. The expanded VPN view dialog box appears.

3. Make the necessary changes, then click OK to apply your changes.

To revert any changes you have made to the VPN, right-click the VPN name in the navigation tree and select Revert Changes.

Editing VPN Protected Resources

To edit a protected resource in the VPN, right-click the protected resource and select Edit Protected Resource. Make your changes, then click OK to save your changes.

If you make changes to a protected resource object that is used in a VPN, NetScreen-Security Manager automatically generates new configuration and propagates your changes to all affected security devices. If you change the security device that protects a resource, NetScreen-Security Manager removes the previous security device from all affected VPNs and adds the new security device.

However, NetScreen-Security Manager does not configure the VPN topology for the new security device—you must reconfigure the topology to include the new device manually.

Editing Users

To edit a user object in the VPN, right-click the user and select Edit Remote User. Make your changes, then click OK to save your changes.

Editing the VPN Configuration

To add or delete a member, edit any VPN parameter, or reconfigure the VPN topology, select the VPN and click OK. Make your changes, then click Save to re-generate the VPN.

---

**NOTE:** After you click Save, you cannot revert your changes to a VPN.

---

Editing VPN Overrides

If you add, edit, or delete an override, the VPN link automatically updates the autogenerated rules to reflect those edits.
VPN Manager Examples

This section provides examples of common VPN types:

- Configuring an AutoKey IKE, Policy-Based Site-to-Site VPN
- Configuring an AutoKey IKE RAS, Policy-Based VPN
- Configuring an AutoKey IKE, Route-Based Site-to-Site VPN
- Configuring XAuth Authentication with External User Group

The following sections provide step-by-step instructions on creating each VPN type.

NOTE: For examples on creating a Manual Key VPN, see “Device-Level VPN Examples” on page 489.

EXAMPLE: CONFIGURING AN AUTOKEY IKE, POLICY-BASED SITE-TO-SITE VPN

An AutoKey IKE VPN connects protected resources using AutoKey IKE. Use this VPN type to connect and control traffic between two security devices.

In this example, an AutoKey IKE tunnel using a pair of certificates (one at each end of the tunnel) provides the secure connection between the Tokyo and Paris offices. For the Phase 1 and 2 security levels, you specify the Phase 1 proposal as rsa-g2-3des-sha and select the predefined “Compatible” set of proposals for Phase 2. It is assumed that both participants already have RSA certificates and are using Entrust as the certificate authority (CA). All zones are in the trust-vr.

Figure 122: Configure AutoKey IKE VPN Example Overview

1. Configure the security devices. For details on adding devices, see Chapter 4, “Adding Devices”.

   a. Configure the Tokyo device with the following interfaces:
Ethernet1 is the Trust IP (10.1.1.1/24) in the Trust zone.
Ethernet3 is the Untrust IP (1.1.1.1/24) in the Untrust zone.

b. Configure the Paris device with the following interfaces:

Ethernet1 is the Trust IP (10.2.2.1/24) in the Trust zone.
Ethernet3 is the Untrust IP (2.2.2.2/24) in the Untrust zone.

2. Create the Address Objects that you will use to create Protected Resources (for details on creating or editing Address Objects, see “Configuring Address Objects” on page 227). If you imported a security device, the address book objects configured on that device are automatically imported as Address Objects into the NetScreen-Security Manager UI.

a. Add the Tokyo Trust LAN (10.1.1.0/24) as a network Address Object. In Address Objects, click the Add icon and select Network. Configure the following, then click OK:

- For Name, enter Tokyo Trust LAN
- For IP Address/Netmask, enter 10.1.1.0/24
- For Color, select magenta.
- For Comment, enter Tokyo Trust Zone.

b. Add the Paris Trust LAN (10.2.2.0/24) as a network Address Object. In Address Objects, click the Add icon and select Network. Configure the following, then click OK:

- For Name, enter Paris Trust LAN
- For IP Address/Netmask, enter 10.2.2.0/24
- For Color, select magenta.
- For Comment, enter Paris Trust Zone.

3. Create the Protected Resources to represent the source and destination points of the VPN. (for details on creating or editing Protected Resources, see “Configuring Protected Resources” on page 313).

a. Create the Tokyo Protected Resources object. In Protected Resources (under VPN Manager), click the Add icon. Configure as shown below, then click OK:
Figure 123: Create Tokyo Protected Resource Object for AutoKey IKE VPN

![Protected Resource Table]  
Name: Tokyo Protected Resources  
Color: green  
Service Object: any  
Server/Client: Both  
Network Object: Tokyo Trust LAN  
Comment:  

<table>
<thead>
<tr>
<th>Security Gateway Device</th>
<th>Zone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tokyo</td>
<td>trust</td>
</tr>
</tbody>
</table>

b. Create the Paris Protected Resources object. In Protected Resources (under VPN Manager), click the Add icon. Configure as shown below, then click OK:

Figure 124: Create Paris Protected Resource Object for AutoKey IKE VPN

![Protected Resource Table]  
Name: Paris Protected Resources  
Color: green  
Service Object: any  
Server/Client: Both  
Network Object: Paris Trust LAN  
Comment:  

<table>
<thead>
<tr>
<th>Security Gateway Device</th>
<th>Zone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paris</td>
<td>trust</td>
</tr>
</tbody>
</table>

4. Create the VPN. In the navigation tree, double-click VPN Manager, then right-click VPNs and select AutoKey IKE VPN. The New AutoKey IKE VPN dialog box appears. Configure the General VPN Properties:

a. In Name, enter Tokyo-Paris Policy-Based VPN.

b. Select Enable.

c. In Termination Point, select Untrust.

d. For VPN Type, select Policy-Based.

e. Click OK to save the VPN and return to VPN Manager.
f. In VPN Manager, select the Tokyo-Paris Policy-Based VPN. The VPN appears in the main display area.

5. Configure the policy-based members:
   a. Select the Protected Resources link to display the Protected Resources list.
   b. Select the Paris Protected Resources and the Tokyo Protected Resources.
   c. Click OK to return to the main display area.

6. Configure the VPN topology:
   a. Select the Topology link to display the Topology dialog box.
   b. Click the Add icon to display the Topology configuration dialog box. Configure the following:
      - For Hub and Supernet, leave the default of none.
      - Enable Mesh Main(s).
      - In the Mains window, select the Paris and Tokyo security devices.
   c. Click OK to return to the Topology dialog box, then click OK to return to the main display area.

7. Configure the termination points of the VPN:
   a. Click the Termination Points link. The Termination Points dialog box appears.
   b. Confirm that both Paris and Tokyo devices use a Termination Interface of ethernet3.
   c. Click OK to return to the main display area.

8. Configure the VPN gateway:
   a. Click the Gateway Parameters link. The Properties tab appears. Leave all defaults and click the Security tab.
   b. In the Security tab, configure the PKI Information and Phase 1 Proposals as shown below:
c. Click Save to save your configuration changes to the VPN.

To view the autogenerated rules, click the Policy Rules link in the Overrides section. VPN Manager generates the rules as shown below:

9. Add the VPN Link. You must create a VPN link between the Zone rulebase in a Security Policy and the VPN Manager autogenerated rules. You create this link by inserting a VPN link in the zone rulebase; this links points to the VPN rules that exist in the VPN Manager.
   
a. In Security Policies, select an existing Security Policy (or create a new Security Policy). In the Zone rulebase, right-click and select Add VPN link.

b. Select the Tokyo-Paris Policy-Based VPN, then click OK to add the link. By default, the link appears at the top of the rulebase, but you can move the VPN link anywhere in the rulebase, just as you would a firewall rule.
EXAMPLE: CONFIGURING AN AUTOKEY IKE RAS, POLICY-BASED VPN

An AutoKey IKE RAS VPN connects RAS users and protected resources. In this example, Local Auth user Wendy (login name: reporter, password: Nd4syst4) wants to access resources on the UNIX server at the corporate site.

To accommodate Wendy, create an AutoKey IKE tunnel using a preshared key to provide the secure communication channel between IKE user Wendy and the UNIX server, which is protected by the Chicago Corporate security device.

The tunnel uses ESP with 3DES encryption and SHA-1 authentication. For the Phase 1 and 2 security levels, specify the Phase 1 proposal as pre-g2-3des-sha and select the predefined “Compatible” set of proposals for Phase 2.

Figure 127: AutoKey IKE RAS VPN Example Overview

1. Add the Chicago Corporate device (for details on adding devices, see Chapter 4, “Adding Devices”) and configure the following interfaces:
   - Ethernet1 is the Trust IP (10.1.1.1/24) in the Trust zone.
   - Ethernet3 is the Untrust IP (1.1.1.1/24) in the Untrust zone.

2. Create the Address Objects that you will use to create Protected Resources (for details on creating or editing Address Objects, see “Configuring Address Objects” on page 227).
   a. Add the Chicago Corporate Trusted LAN (10.1.1.0/24) as an network Address Object. In Address Objects, click the Add icon and select Network. Configure the following, then click OK:
      - For Name, enter Chicago Corporate Trust LAN.
      - For IP Address/Netmask, enter 10.2.1.0/24.
      - For Color, select magenta.
      - For Comments, enter Chicago Trusted Network.
   b. Add the UNIX Server (10.1.1.5) as a host Address Object. In Address Objects, click the Add icon and select Host. Configure the following, then click OK:
3. Create Chicago Corporate Trusted LAN Protected Resources to represent the destination point of the VPN (for details on creating Protected Resources, see “Configuring Protected Resources” on page 313). In Protected Resources (under VPN Manager), click the Add icon. Configure as shown below, then click OK:

![Figure 128: Add Chicago Protected Resource for AutoKey IKE RAS VPN](image)

4. Create a Local User Object to represent Wendy, the remote user (for details on creating User Objects, see “Configuring User Objects” on page 298). Local User objects are authenticated with the local NetScreen-Security Manager database.

   a. In User Objects, select Local User Objects. In the main display area, click the Add icon and select Local. Configure as shown below, then click OK:
5. Create the VPN. In the navigation tree, double-click VPN Manager, then right-click VPNs and select AutoKey IKE RAS VPN. The New AutoKey IKE RAS VPN dialog box appears. Configure as shown below:

a. For Name, enter UNIX Remote Access VPN.

b. Select Enable.

c. In Termination Point, select Untrust.

d. Click OK to save the VPN and return to VPN Manager. In VPN Manager, select the UNIX Remote Access VPN.

6. Configure the policy-based members:

a. In the main display area, select the Protected Resources link.

b. In the Protected Resources list, select the Chicago Corporate Trusted LAN, then click OK to return to the main display area.

7. Configure the termination points of the VPN:

a. Click the Termination Points link. The Termination Points dialog box appears.

b. Configure Chicago Corporate to use ethernet3 as the termination point (this is the Untrust interface), then click OK to return to the main display area.
8. Configure the remote users for the VPN:
   a. In the Remote Users section, click the Users link. The Remote User dialog box appears.
   b. Select the user “wparker”, then click Save to save your configuration changes to the VPN.

9. Configure the VPN gateway:
   a. Click the Gateway Parameters link. The Properties tab appears. Leave all defaults and click the Security tab.
   b. In the Security tab, enter the preshared key value (h1p8A24nG5), then click Generate Key.
   c. For Phase 1 Proposals, select User-Defined, then click the Add/Edit icon to add the pre-g2-3des-sha proposal, as shown below:

   Figure 130: Configure Security for AutoKey IKE RAS VPN

   d. Click Save to save your configuration changes to the VPN.

   To view the autogenerated rules, click the Policy Rules link in the Overrides section. VPN Manager generates the rules as shown below:

   Figure 131: View Autogenerated Rules for AutoKey IKE RAS VPN
10. Add the VPN Link. You must create a VPN link between the Security Policy and the VPN Manager autogenerated rules. You create this link by inserting a VPN link in the Security Policy; this links points to the VPN rules that exist in the VPN Manager.


   b. Select the UNIX Remote Access VPN.

   c. Click OK to add the link to the policy. By default, the link appears at the top of the policy, but you can move the VPN link anywhere in the policy, just as you would a firewall rule.

EXAMPLE: CONFIGURING AN AUTOKEY IKE, ROUTE-BASED SITE-TO-SITE VPN
In this example, an AutoKey IKE VPN tunnel using a preshared key provides a secure connection between security devices protecting the Tokyo and Paris offices. The Untrust zone interface for both security devices use a static IP address. All security and tunnel zones are in the trust-vr. The preshared key is h1p8A24nG5. For the Phase 1 and 2 security levels, specify the Phase 1 proposal as pre-g2-3des-sha and the Phase 2 proposal as predefined compatible.

Figure 132: AutoKey IKE, RB Site-to Site VPN Example Overview

1. Add the Tokyo and Paris security devices (for details on adding devices, see Chapter 4, “Adding Devices”):

   a. Configure the Tokyo device with the following interfaces:

      ■ Ethernet1 is the Trust IP (10.1.1.1/24) in the Trust zone.

      ■ Ethernet3 is the Untrust IP (1.1.1.1/24).

   b. Configure the Paris device with the following interfaces:

      ■ Ethernet1 is the Trust IP (10.2.2.1/24) in the Trust zone.
Ethernet3 is the Untrust IP (2.2.2.2/24) in the Untrust zone.

2. Create the Address Objects that you use for the VPN rule in the firewall rulebase (for details on creating VPN rules, see “Adding VPN Rules” on page 488).

   a. Add the Tokyo Trust LAN (10.1.1.0/24) as an network Address Object. In Address Objects, click the Add icon and select Network. Configure the following, then click OK:
      - For Name, enter Tokyo Trust LAN
      - For IP Address/Netmask, enter 10.1.1.0/24
      - For Color, select magenta.
      - For Comment, enter Tokyo Trust Zone.

   b. Add the Paris Trust LAN (10.2.2.0/24) as a network Address Object. In Address Objects, click the Add icon and select Network. Configure the following, then click OK:
      - For Name, enter Paris Trust LAN
      - For IP Address/Netmask, enter 10.2.2.0/24
      - For Color, select magenta.
      - For Comment, enter Paris Trust Zone.

3. Create the VPN. In the navigation tree, double-click VPN Manager, right-click VPNs and select AutoKey IKE VPN. The New AutoKey IKE VPN dialog box appears. Configure as shown below:

   a. In Name, enter Tokyo-Paris Route-based VPNs.

   b. Select Enable.

   c. In Termination Point, select Untrust.

   d. Click OK to save the VPN and return to VPN Manager. In VPN Manager, select the Tokyo-Paris Route-based VPNs.

4. Configure the route-based members:

   a. In the main display area, select the security device link (under Route-Based Configuration) to display the zone and tunnel options. Configure the default zone and tunnel options as shown below:
VPN Manager Examples

Chapter 10: Configuring VPNs

Figure 133: Configure Members for AutoKey IKE, RB Site-to-Site VPN

Select Devices

<table>
<thead>
<tr>
<th>Primary Zone</th>
<th>untrust</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secondary Zone</td>
<td>untrust</td>
</tr>
<tr>
<td>Physical Source Interface Zone</td>
<td>untrust</td>
</tr>
</tbody>
</table>

Tunnel Options

- Generate Single Tunnel Interface for 5.0 devices
- Generate NHTB entries for 5.0 devices

b. Click the Add icon to display available security devices. Select the Paris and Tokyo devices.

c. Click OK to add the members to the VPN.

d. Ensure that the route-based members are configured as shown below:

Figure 134: View Members for AutoKey IKE, RB Site-to-Site VPN

<table>
<thead>
<tr>
<th>Firewall Device</th>
<th>Tunnel Interface Zone</th>
<th>Physical Source Interface</th>
<th>Single Tunnel Interface</th>
<th>NHTB entries</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paris</td>
<td>untrust</td>
<td>ethernet3</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Tokyo</td>
<td>untrust</td>
<td>ethernet3</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

e. Click OK to save your settings and return to the main display area.

5. Configure the VPN topology:

a. Select the Topology link. The Topology dialog box appears.
b. Click the Add icon to display the Topology configuration dialog box.
c. In the Mains window, select the Paris and Tokyo security devices.
d. Click OK to return to the Topology dialog box, then click OK to return to the main display area.

6. Configure the termination points of the VPN:

a. Click the Termination Points link. The Termination Points dialog box appears.
b. Confirm that both Paris and Tokyo devices use a Termination Interface of ethernet3, then click OK to return to the main display area.

7. Configure the VPN gateway:

a. Click the Gateway Parameters link. The Properties tab appears. Leave all defaults and click the Security tab.
b. In the Security tab, enter the preshared key value (h1p8A24nG5), then click Generate Key.

c. For Phase 1 Proposals, select User-Defined, then click the Add/Edit icon to add the pre-g2-3des-sha proposal, as shown below:

Figure 135: Configure Security for AutoKey IKE, RB Site-to Site VPN

<table>
<thead>
<tr>
<th>Properties</th>
<th>Security</th>
<th>IKE IDs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preshare Key/RSA/D5A</td>
<td>![Preshare Key Information]</td>
<td></td>
</tr>
<tr>
<td>![Generate Key]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Preshared Key</td>
<td>**********************************</td>
<td></td>
</tr>
<tr>
<td>Phase 1 Proposals</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Level</td>
<td>![User-Defined]</td>
<td></td>
</tr>
<tr>
<td>![ pre-g2-3des-sha]</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

8. Click Save to save your configuration changes to the VPN. Because this VPN is route-based, no rules are autogenerated. However, you can view the device tunnel summary to see all autogenerated tunnels between each security device in the VPN, as shown below:

Figure 136: View Tunnel Summary for AutoKey IKE, RB Site-to Site VPN

<table>
<thead>
<tr>
<th>AutoKey IKE VPN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Please make sure to Save after Configuration Changes to view correct data</td>
</tr>
<tr>
<td>Source Device / Peer Device</td>
</tr>
<tr>
<td>---------</td>
</tr>
<tr>
<td>Paris</td>
</tr>
<tr>
<td>Tokyo</td>
</tr>
</tbody>
</table>

A tunnel interface acts as a doorway to a VPN tunnel; traffic enters and exits a VPN tunnel via a tunnel interface. These tunnels are an “always-on” connection—the devices will route any traffic with an appropriate source and destination IP address through the VPN tunnel.

To control traffic through the tunnel, you must add firewall rules to the Security Policy that is installed on each VPN node. For details on creating firewall rules, see “Configuring Firewall Rules” on page 330.
Next, you must create the routes (in the route table of each device) that will connect the autogenerated tunnel interfaces and form the VPN tunnel (for details on creating routes, see "NetScreen-Security Manager: Configuring Firewall/VPN 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.

9. Configure the route on the Tokyo security device.

   a. In Device Manager, double-click the device to open the device configuration dialog box. Select Network > Virtual Router to display the list of virtual routers on the device.

   b. Double-click the trust-vr route to open the vr for editing. In the virtual router dialog box, click Routing Table, then click the add icon under destination-based Routing Table to add a new static route.

   c. Configure a route from the untrust interface to the gateway, as shown below:

   **Figure 137: Configure Untrust Route for AutoKey IKE, RB Site-to Site VPN**

    ![New Routing Table](image)

   **NOTE:** ScreenOS 4.0.x devices display only the destination-based Routing Table; ScreenOS 5.x devices display both destination-based and source-based routing tables.
d. Configure route from the trust zone to the tunnel interface, as shown below:

Figure 138: Configure Trust Route for AutoKey IKE, RB Site-to Site VPN

![New Routing Table](image)

Your routing table should appear as shown below:

Figure 139: View Routing Table for AutoKey IKE, RB Site-to Site VPN

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Mask</th>
<th>Next Hop</th>
<th>Vsys</th>
</tr>
</thead>
</table>
| 0.0.0.0    | 0    | Interface: ethernet3  
Gateway IP Address: 1.1.1.250  
Metric: 1  
Tag: | ... |
| 10.2.2.0   | 24   | Interface: tunnel.1  
Gateway IP Address: 0.0.0.0  
Metric: 1  
Tag: | ... |

e. Click OK to save your changes to the virtual router, then click OK to save your changes to the Tokyo device.

10. Configure the route on the Paris security device:

a. In Device Manager, double-click the device to open the device configuration dialog box. Select Network > Virtual Router to display the list of virtual routers on the device.
b. Double-click the trust-vr route to open the vr for editing. In the virtual router dialog box, click Routing Table, then click the add icon under destination-based Routing Table to add a new static route.

NOTE: ScreenOS 4.0.x devices display only the destination-based Routing Table; ScreenOS 5.x devices display both destination-based and source-based routing tables.

c. Configure a route from the untrust interface to the gateway, as shown below:

Figure 140: Configure Untrust Route for AutoKey IKE, RB Site-to Site VPN

![New Routing Table](image)

- IP Address: 0.0.0.0
- Network Mask: 0
- Next Hop: Gateway
- Interface: ethernet3
- Gateway IP Address: 2.2.2.250
- Metric: 1
- Tag: none

- [OK] - [Cancel]

d. Configure route from the trust zone to the tunnel interface, as shown below:

Figure 141: Configure Trust Route for AutoKey IKE, RB Site-to Site VPN

![New Routing Table](image)

- IP Address: 10.1.1.0
- Network Mask: 24
- Next Hop: Gateway
- Interface: tunnel1
- Gateway IP Address: 0.0.0.0
- Metric: 1
- Tag: none

- [OK] - [Cancel]
Your routing table should appear as shown below:

Figure 142: View Routing Table for AutoKey IKE, RB Site-to Site VPN

<table>
<thead>
<tr>
<th>Destination-based Routing Table</th>
</tr>
</thead>
<tbody>
<tr>
<td>+</td>
</tr>
<tr>
<td>IP Address</td>
</tr>
</tbody>
</table>
| 0.0.0.0     | 0    | Interface: ethernet3  
            |       |         |      |
|            |      | Gateway IP Address: 2.2.2.250  
            |       | Metric: 1  
            |       | Tag: ... |
| 10.1.1.0    | 24   | Interface: tunnel 1  
            |       | Gateway IP Address: 0.0.0.0  
            |       | Metric: 1  
            |       | Tag: ... |

e. Click OK to save your changes to the virtual router, then click OK to save your changes to the Paris device.

EXAMPLE: CONFIGURING XAUTH AUTHENTICATION WITH EXTERNAL USER GROUP

In this example, you use a VPN to enable access for a group of resellers who require access to FTP servers in the corporate LAN. First, you must configure the RADIUS server using the custom port 4500 (default is 1645), then add an authentication server object in NetScreen-Security Manager to represent that server.

Next, to manage the users in this example, you define an external user group in two places: on the external RADIUS auth server and in NetScreen-Security Manager.

- On the RADIUS server, you populate the external user group with XAuth users, leaving the group unpopulated in NetScreen-Security Manager. The RADIUS server authenticates the users during Phase 1 IKE negotiations.

- In NetScreen-Security Manager, you leave the external user group unpopulated, but you must define each user as a local user with an IKE ID, then create a group that includes those local users as members. This IKE ID is used to authenticate the users during the Phase 2 IKE negotiations.

Additionally, you must add the security device and create an Address object to represent the FTP server, as well as a protected resource. After you have assembled all the VPN components, you are ready to create the VPN.

1. Configure the RADIUS Server. On the RADIUS server, load the Juniper Networks dictionary file and define Xauth user accounts. Use the Juniper Networks user group VSA to create the user group xa_grp2 and apply it to the auth user accounts that you want to add to that group.

NOTE: For instructions on loading the dictionary file onto a RADIUS server, refer to the RADIUS server documentation. If you are using a Microsoft IAS RADIUS server, there is no dictionary file to load. Instead, define the correct vendor-specific attributes (VSAs) on the server.
2. Configure the VPN Components:

a. Add the Authentication Server Object. In the main navigation tree, select Object Manager > Authentication Servers and click the Add icon. Configure the following, then click OK:
   - For name, enter radius1. Select a color and add a comment, if desired.
   - For Main Server, enter the IP 10.20.1.100; for Primary Backup Server, enter IP 10.20.1.110; for Secondary Backup Server, enter IP 10.20.1.120.
   - For timeout, enter 30.
   - Enable For XAuth Users.
   - For Server Type, select RADIUS, then configure the RADIUS server:
     - For server port, select 4500 (default is 1645)
     - For secret, enter A56hYY97kl
     - For retry timeout, enter 4.

b. Add an External User Group (in NetScreen-Security Manager). In the Object Manager, select User Objects > External User Groups. Click the Add icon to display the New External User Group dialog box. Configure the following, then click OK:
   - For Name, enter xa-grp2.
   - For Color, select yellow.
   - For Comment, enter Reseller Group RADIUS.
   - Enable XAuth.

c. Add the Local User Object. In the Object Manager, select User Objects > Local Users. Click the Add icon and select User. The New Local User dialog box appears. Configure the following, then click OK.
   - For Name, enter jhansen.
   - For Color, select orange.
   - For Comment, enter reseller group.
   - Select Enable, then select IKE.
   - For IKE settings, enable User FQDN and enter the email address jhansen@company.com.

d. Add a Local User Group. In the Object Manager, select User Objects > Local User Groups. Click the Add icon to display the New Local User Group dialog box. Configure the following, then click OK:
For Name, enter Reseller User Group.

For color, enter green.

For Comment, enter Reseller VPN XAuth RADIUS.

Add jhansen as a member.

e. Add a Network address object to represent the network used by Reseller group. In the Object Manager, select Address Objects, then click the Add icon and select Network. The New Network dialog box appears. Configure the following, then click OK:

   - For Name, enter reseller1.
   - For IP Address/Netmask, enter 10.2.2.0/24.
   - For color, select cyan.
   - For Comment, enter Reseller Group.

f. Add an Address Object to represent the FTP Server. In the Object Manager, select Address Objects, then click the Add icon and select Host. The New Host dialog box appears. Configure the following, then click OK:

   - For Name, enter rsl-svr1.
   - For Color, select green.
   - For Comment, enter FTP Server.
   - Select IP, then enter the IP Address 10.1.1.5.

g. Add a NetScreen-208 security device named “Bozeman”. This is the device protects the FTP server (for details on adding devices, see Chapter 4, “Adding Devices”). Configure the Bozeman device with the following interfaces:

   - Ethernet1 is the Trust IP (10.1.1.1/24) in the Trust zone.
   - Ethernet3 is the Untrust IP (2.2.2.2/24) in the Untrust zone.

h. Create a Protected Resource to represent the destination point of the VPN (for details on creating Protected Resources, see “Configuring Protected Resources” on page 313). In this example, the destination point is the FTP server in the trust zone of Bozeman. In Protected Resources (under VPN Manager), click the Add icon. Configure the object as shown below, then click OK:
Chapter 10: Configuring VPNs

3. Create the VPN. In the main navigation tree, select VPN Manager > VPNs. Click the Add icon and select AutoKey IKE RAS VPN. The New AutoKey IKE RAS VPN dialog box appears. Configure as shown below:
   a. In Name, enter Reseller Remote Access VPN.
   b. Select Enable.
   c. In Termination Point, select Untrust.
   d. Click OK to save the VPN and return to VPN Manager. The Reseller Remote Access VPN appears in the main display area.

4. Configure the policy-based members:
   a. In the main display area, select the Protected Resources link.
   b. In the Protected Resources list, select the rsl-svr1 protected resource, then click OK:

5. Configure the termination points of the VPN:
   a. Click the Termination Points link. The Termination Points dialog box appears.
   b. Configure the Bozeman device to use ethernet3 as the termination point (this is the Untrust zone interface).
c. Click OK to return to the main display area.

6. Configure the remote users for the VPN:
   a. In the Remote Users section, click the Users link. The Remote User dialog box appears.
   b. Select the Reseller local user group as shown below:

   Figure 144: Configure Remote User (Reseller Local User Group)

   c. Click Save to save your configuration changes to the VPN.

7. Configure the VPN gateway:
   a. Click the Gateway Parameters link. The Properties tab appears.
   b. For Mode, select Main.
   c. In the XAuth section, select XAuth Server and then select the radius1 authentication server for Auth Server Name. Later, after you have autogenerated the VPN rules and gateway, you can override this setting to include only the Reseller external user group. For details, see “Configure Overrides. By default, the gateway attempts to authenticate all users using the specified authentication server (radius1). You must override the gateway security settings to enable the VPN to authenticate only the Reseller external user group:” on page 473.
   d. In the Security tab, enter the preshared key value (netscreen4), then click Generate Key.
   e. For Phase 1 Proposals, select User-Defined, then click the Add/Edit icon to add the pre-g2-3des-sha proposal, as shown below:
f. Click Ok to save your changes to the gateway.

8. Click Save to save your configuration changes to the VPN and autogenerate the policy rules.

To view the autogenerated rules, click the Policy Rules link in the Overrides section. VPN Manager generates the rules as shown below:

9. Configure Overrides. By default, the gateway attempts to authenticate all users using the specified authentication server (radius1). You must override the gateway security settings to enable the VPN to authenticate only the Reseller external user group:

a. In the overrides area, click the Device Configuration link.

b. In the navigation tree, double-click Bozeman and select Gateway. The autogenerated gateway for the Bozeman appears in the main display area.

c. Right-click the autogenerated gateway and select Edit. The Properties tab appears.

d. In the IKE IDs/XAuth tab, configure the XAuth area to authenticate only the Reseller external group, as shown below:
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 475.

- 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 482.

- 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 486.
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 487.

**Supported Configurations**

IKE VPNs support tunnel mode, and can be policy-based or route-based; however, route-based VPNs do not support RAS users.

L2TP VPNs support transport mode, and can be policy-based.

**Creating AutoKey IKE VPNs**

Creating device-level AutoKey IKE VPNs is a four stage process:

- Configure Gateway
- Configure Routes (Route-based only)
- Configure VPN on the Device
- Add VPN rules to Security Policy

**Configuring Gateways**

A gateway is an interface on your security device that sends and receives traffic; a remote gateway is an interface on another device that handles traffic for that device. Each security device member has a remote gateway that it sends and receives VPN traffic to and from. To configure a gateway for a VPN member, you need to define the local gateway (the interface on the VPN member that handles VPN traffic) and the remote gateway (the interface on the other VPN member that handles VPN traffic). The interface can be physical or virtual.

- For remote gateways that use static IP addresses, specify the IP address or host name of the remote device.
- For remote gateways that use dynamic IP addresses, configure an IKE ID for the remote device.
- For remote gateways that are RAS users, specify a Local User object as a remote gateway to enable RAS user access.

To add a gateway to a security device, open the device configuration, select VPN Settings, and click the Add icon to display the New Gateway Dialog box. Configure the gateway as detailed in the following sections.

**Properties**

Enter a name for the new gateway, then specify the following gateway values:

- Mode—The mode determines how Phase 1 negotiations occur.
In Main mode, the IKE identity of each node is protected. Each node sends three two-way messages (six messages total); the first two messages negotiate encryption and authentication algorithms that protect subsequent messages, including the IKE identity exchange between the nodes. Depending on the speed of your network connection and the encryption and authentication algorithms you use, main mode negotiations can take a long time to complete. Use Main mode when security is more important.

In Aggressive mode, the IKE identity of each node is not protected. The initiating node sends two messages and the receiving node sends one (three messages total); all messages are sent in the clear, including the IKE identity exchange between the nodes. Because Aggressive mode is typically faster but less secure than Main mode, use Aggressive mode when speed is more important than security. However, you must use Aggressive mode for VPNs that include RAS users.

Remote Gateway—The remote gateway is the VPN gateway on the receiving VPN node, and can be an interface with a static or dynamic IP address, or local or external user object.

Static IP Address. For remote gateways that use a static IP address, enter the IP address and mask.

RAS User/Group. For remote gateways that are users, select the User object or User Group object that represents the RAS user.

Dynamic IP Address. For remote gateways that use a dynamic IP address, select dynamic IP address.

Outgoing Interface—The outgoing interface (also known as the termination interface) is the interface on the security device that sends and receives VPN traffic. Typically, the outgoing interface is in the untrust zone.

Heartbeats—Use heartbeats to enable redundant gateways. You can use the default or set your own thresholds:

Hello. Enter the number of seconds the security device waits between sending hello pulses.

Reconnect. Enter the maximum number of seconds the security device waits for a reply to the hello pulse.

Threshold. Enter the number of seconds that the security device waits before attempting to reconnect.

NAT Traversal—Because NAT obscures the IP address in some IPSec packet headers, a VPN node cannot receive VPN traffic that passes through an external NAT device. To enable VPN traffic to traverse a NAT device, you can use NAT Traversal (NAT-T) to encapsulate the VPN packets in UDP. If a VPN node with NAT-T enabled detects an external NAT device, it checks every VPN packet to determine if NAT-T is necessary. Because checking every packet impacts VPN performance, you should only use NAT Traversal for remote users that must connect to the VPN over an external NAT device.
You do not need to enable NAT-T for your internal security device nodes that use NAT; each VPN node knows the correct address translations for VPN traffic and does not need to encapsulate the traffic.

To use NAT-T, enable NAT-Traversal and specify:

- **UDP Checksum.** A 2-byte value (calculated from the UDP header, footer, and other UDP message fields) that verifies packet integrity. You must enable this option for NAT devices that require UDP checksum verification; however, most NAT devices (including security devices) do not require it.

- **Keep alive Frequency.** The number of seconds a VPN node waits between sending empty UDP packets through the NAT device. A NAT device keeps translated IP addresses active only during traffic flow, and invalidates unused IP addresses. To ensure that the VPN tunnel remains open, you can configure the VPN node to send empty “keep alive” packets through the NAT device.

**IKE IDs/XAuth**

Every VPN member has a unique identification number, known as an IKE ID. During Phase 1 negotiations, the IKE protocol uses the ID to authenticate the VPN member. You must select and configure an ID type for the VPN members at each end of the tunnel. However, the ID type can be different for each member:

- **ASN1-DN**—Abstract Syntax Notation, version 1 is a data representation format that is non-platform specific; Distinguished Name is the name of the computer. Use ASN1-DN to create a Group ID that enables multiple RAS users to connect to the VPN tunnel concurrently.

- At the peer ID, specify values for the Container Match and Wildcard Match.

- At the local ID, specify the value.

Using a Group ID can make configuring and maintaining your VPN quicker and easier. For details on how Group IKE IDs work, see “Configuring Group IKE IDs” on page 431. For details on determining the ASN1-DN container and wildcard values for Group IKE IDs, see Juniper Networks ScreenOS 5.x Concepts and Examples Guide.

- **FQDN**—Use a Fully Qualified Domain Name when the VPN member uses a dynamic IP address. FQDN is a name that identifies (qualifies) a computer to the DNS protocol using the computer name and the domain name; ex. server1.colorado.mycompany.com.

- **IP Address**—Use an IP address when the VPN member uses a static IP address.

- **U-FQDN**—Use a User Fully Qualified Domain Name when the VPN member uses a dynamic IP address (such as a RAS user). A U-FQDN is an email address, such as user1@mycompany.com.

Use the XAuth protocol to authenticate RAS users with an authentication token (such as SecureID) and to make TCP/IP settings (IP address, DNS server, and WINS server) for the peer gateway.
- Default Server—Use the default server to use the default XAuthentication server for the device. To change or assign a default XAuthentication server, edit the VPN settings > Defaults > Xauth settings.

- XAuth Server—Use to specify the authentication server that assigns TCP/IP settings to the remote gateway.
  - XAuth Server Name. Select a pre-configured authentication server object. For details on creating authentication server objects, see “Configuring Authentication Servers” on page 289.
  - Allowed Authentication Type. Select generic or Challenge Handshake Authentication Protocol (CHAP) (password is sent in the clear) to authenticate the remote gateway.
  - Query Remote Setting. Enable this option to query the remote settings object for DNS and WINS information.
  - Users and Groups. To authenticate XAuth RAS users using the authentication server, enable User or User Group and select a preconfigured user object.

- XAuth Client—Use when the remote gateway is a RAS user that you want to authenticate.
  - Allowed Authentication Type. Select Any or Challenge Handshake Authentication Protocol (CHAP) for authentication (password is sent in the clear).
  - User Name and Password. Enter the user name and password that the RAS user must provide for authentication.

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

- Bypass Authentication—Use to permit VPN traffic from this VPN member to pass unauthenticated by the Auth server.

**Security**
Select the authentication method you want to use in the VPN:

- Preshared Key—Use if your VPN includes security devices and/or RAS users. VPN nodes use the preshared key during Phase 1 negotiations to authenticate each other; because each node knows the key in advance, negotiations use fewer messages and are quicker.
To generate a random key, enter a value for the seed, then click Generate Key. NetScreen-Security Manager uses the seed value to generate a random key, which is used to authenticate VPN members.

NOTE: Using a random key can generate a value in excess of 255 characters, which exceeds ScreenOS limits and might not be accepted by the security device during update. To reduce the key size, shorten the autogenerated key value by deleting characters.

To use a predefined value for the key, enter a value for the Preshared Key.

PKI—Use if your VPN includes extranet devices or you require the additional security provided by certificates (PKI uses certificates for VPN member authentication). For details on creating and managing certificates, see “Configuring Certificate Authorities” on page 309.

For Phase 1 negotiations, select a proposal or proposal set. You can select from predefined or user-defined proposals:

- To use a predefined proposal set, select one of the following:
  - Basic (nopfs-esp-des-sha, nopfs-esp-des-md5)
  - Compatible (nopfs-esp-3des-sha, nopfs-esp-3des-md5, nopfs-esp-des-sha, nopfs-esp-des-md5)
  - Standard (gs-esp-3des-sha, gs-esp-aes128-sha)

NOTE: You cannot use a predefined proposal set with certificates—you must select a user-defined proposal or change the authentication method to Preshared Key.

- To use a user-defined proposal, select a single proposal from the list of predefined and custom IKE Phase 1 Proposals. For details on custom IKE proposals, see “Configuring IKE Proposals” on page 316.

If your VPN includes only security devices, you can specify one predefined or custom proposal that NetScreen-Security Manager propagates to all nodes in the VPN. If your VPN includes extranet devices, you should use multiple proposals to increase security and ensure compatibility.

Configuring Routes (Route-based only)

For a routing-based VPN member, you must configure:

- Tunnel zone or tunnel interfaces on the member.
- Static or dynamic routes from the member to other VPN members.

VPN traffic flows through the tunnel zones or tunnel interfaces on the security device, and uses static or dynamic routes to reach other VPN members. You must create the tunnel zones and interfaces before configuring routes.
For details on configuring tunnel zones, tunnel interfaces, static routes, or dynamic routes, see “NetScreen-Security Manager: Configuring Firewall/VPN Devices”.

After you have configured the tunnel zone or interface on the security device, you must bind the VPN to that zone or interface to make the VPN functional, as described in the following section.

Configuring the VPN

When you configure the VPN, you are defining the gateway the security device uses to connect to the VPN, the IKE Phase 2 proposals used by that gateway, and how you want NetScreen-Security Manager to monitor the VPN tunnel.

For route-based VPNs, you are also binding the VPN to the tunnel interface or zone that sends and receives VPN traffic to and from the device.

Properties

Enter the following values:

- **VPN name**—Enter a name for the VPN.

- **Remote Gateway**—Select the gateway for the VPN.

- **Idle Time to Disable SA**—Configure the number of minutes before a session that has no traffic automatically disables the SA.

- **Replay Protection**—In a replay attack, an attacker intercepts a series of legitimate packets and uses them to create a denial-of-service (DoS) against the packet destination or to gain entry to trusted networks. If replay protection is enabled, your security devices inspect every IPSec packet to see if the packet has been received before—if packets arrive outside a specified sequence range, the security device rejects them.

- **IPSec Mode**—Configure the mode:
  - Use tunnel mode for IPSec. Before an IP packet enters the VPN tunnel, NetScreen-Security Manager encapsulates the packet in the payload of another IP packet and attaches a new IP header. This new IP packet can be authenticated, encrypted, or both.
  - Use transport mode for L2TP-over-IPSec. NetScreen-Security Manager does not encapsulate the IP packet, meaning that the original IP header must remain in plaintext. However, the original IP packet can be authenticated, and the payload can be encrypted.
  - Do not set Fragment Bit in the Outer Header—The Fragment Bit controls how the IP packet is fragmented when traveling across networks.
    - **Clear**. Use this option to enable IP packets to be fragmented.
    - **Set**. Use this option to ensure that IP packets are not fragmented.
    - **Copy**. Select to use the same option as specified in the internal IP header of the original packet.
Security
For Phase 2 negotiations, select a proposal or proposal set. You can select from predefined or user-defined proposals:

- To use a predefined proposal set, select one of the following:
  - Basic (nopfs-esp-des-sha, nopfs-esp-des-md5)
  - Compatible (nopfs-esp-3des-sha, nopfs-esp-3des-md5, nopfs-esp-des-sha, nopfs-esp-des-md5)
  - Standard (gs-esp-3des-sha, gs-esp-aes128-sha)

- To use a user-defined proposal, select a single proposal from the list of predefined and custom IKE Phase 2 Proposals. For details on custom IKE proposals, see “Configuring IKE Proposals” on page 316.

If your VPN includes only security devices, you can specify one predefined or custom proposal that NetScreen-Security Manager propagates to all nodes in the VPN. If your VPN includes extranet devices, you should use multiple proposals to increase security and ensure compatibility.

Binding/ProxyID
You can bind the VPN tunnel to a tunnel interface or tunnel zone to increase the number of available interfaces in the security device. To use a tunnel interface and/or tunnel zone in your VPN, you must first create the tunnel interface or zone on the device; for details, see “Configuring Tunnel Interfaces and Tunnel Zones” on page 431 and “NetScreen-Security Manager: Configuring Firewall/VPN 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 security device to bind the VPN tunnel to the tunnel interface. The security device routes all VPN traffic through the tunnel interface to the protected resources.
- Tunnel Zone—Select a pre-configured tunnel zone on the security device to bind the VPN tunnel directly to the tunnel zone. The tunnel zone must include one or more numbered tunnel interfaces; when the security device routes VPN traffic to the tunnel zone, the traffic uses one or more of the tunnel interfaces to reach the protected resources.

You can also enable proxy and configure the proxy parameters.

Monitor
You can enable VPN Monitor and configure the monitoring parameters for the device. Monitoring is off by default. To enable the VPN Monitor in Realtime Monitor to display statistics for the VPN tunnel, configure the following:
VPN Monitor—When enabled, the device sends ICMP echo requests (pings) through the tunnel at specified intervals (configurable in seconds) to monitor network connectivity (the device uses the IP address of the local outgoing interface as the source address and the IP address of the remote gateway as the destination address). If the ping activity indicates that the VPN monitoring status has changed, the device triggers an SNMP trap; VPN Monitor (in RealTime Monitor) tracks these SNMP statistics for VPN traffic in the tunnel and displays the tunnel status.

Rekey—When enabled, the device regenerates the IKE key after a failed VPN tunnel attempts to re-establish itself. When disabled, the device monitors the tunnel only when the VPN passes user-generated traffic (instead of using device-generated ICMP echo requests). Use the rekey option to:

- Keep the VPN tunnel up even when traffic is not passing through
- Monitor devices at the remote site.
- Enable dynamic routing protocols to learn routes at a remote site and transmit messages through the tunnel.
- Automatically populate the next-hop tunnel binding table (NHTB table) and the route table when multiple VPN tunnels are bound to a single tunnel interface.

Optimized—(This option appears only for devices running ScreenOS 5.x.) When enabled, the device optimizes its VPN monitoring behavior as follows:

- Considers incoming traffic in the VPN tunnel as ICMP echo replies. This reduces false alarms that might occur when traffic through the tunnel is heavy and the echo replies cannot get through.
- Suppresses VPN monitoring pings when the tunnel passes both incoming and outgoing traffic. This can help reduce network traffic.

Source Interface and Destination IP—Configure these options to use VPN Monitoring when the other end of the VPN tunnel is not a security device. Specify the source and destination IP addresses.

Adding a VPN Rule
After you have configured the VPN on each device you want to include in the VPN, you can add a VPN rule to a Security Policy:

- For policy-based VPNs, you must add a VPN rule to create the VPN tunnel.
- For route-based VPNs, the VPN tunnel is already in place. However, you might want to add a VPN rule to control traffic through the tunnel.

For details on adding and configuring a VPN rule in a Security Policy, see “Adding VPN Rules” on page 488.

**Creating Manual Key VPNs**
Creating a device-level Manual Key VPN is a four stage process:
1. Configure XAuth Users
2. Configure Routes (Route-based only)
3. Configure VPN on Device
4. Add VPN rules to Security Policy

Adding XAuth Users
For VPNs that use IPSec manual key to provide remote access services, you must add an XAuth User to the security device. An XAuth User has an account on the security device that guards the protected resources in the VPN; when the user attempts to connect to a protected resource, the security device authenticates the user.

To add a XAuth User for a security device, in the security device configuration L2TP/XAuth/Local User, click the Add icon. Enter a name for the user, then specify:

- User—Select a preconfigured Local User object that is configured for XAuth.
- Remote Setting—Select a preconfigured Remote Settings object.
- IP Pool—Select a preconfigured IP Pool object.
- Static IP—Enter the static IP address of the Local User.

Configuring Routes (Route-based only)
For a routing-based VPN member, you must configure:

- Tunnel zone or tunnel interfaces on the member.
- Static or dynamic routes from the member to other VPN members.

VPN traffic flows through the tunnel zones or tunnel interfaces on the security device, and uses static or dynamic routes to reach other VPN members. You must create the tunnel zones and interfaces before configuring routes. For details on configuring tunnel zones, tunnel interfaces, and static or dynamic routes, see “NetScreen-Security Manager: Configuring Firewall/VPN Devices”.

After you have configured the tunnel zone or interface on the security device, you must bind the VPN to that zone or interface to make the VPN functional, as described in the following section.

Configuring the VPN
The following sections detail how to configure the VPN.

Properties
Enter the following values:

- VPN name—Enter a name for the VPN.
- Gateway—Enter a gateway for the VPN.
- Local SPI—The local Security Parameter Index.
- Remote SPI—The remote Security Parameter Index.
- Outgoing Interface—The outgoing interface is the interface on the security device that sends and receives VPN traffic. Typically, the outgoing interface is in the untrust zone.
- Do not set Fragment Bit in the Outer Header—The Fragment Bit controls how the IP packet is fragmented when traveling across networks.
  - Clear. Use this option to enable IP packets to be fragmented.
  - Set. Use this option to ensure that IP packets are not fragmented.
  - Copy. Select to use the same option as specified in the internal IP header of the original packet.
- IPSec Protocol—Specify the IPSec protocol and algorithm you want to use for data authentication and/or encryption. Because this information is static for each VPN member, they do not need to negotiate for communication.
  - AH. Use Authentication Header to authenticate the VPN traffic, but not encrypt the traffic. If you select AH, you must also specify the key or password that AH uses in the authentication algorithm.

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

- 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 security device. To use a tunnel interface and/or tunnel zone in your VPN, you must first create the tunnel interface or zone on the device; for details, see “Configuring Tunnel Interfaces and Tunnel Zones” and “NetScreen-Security Manager: Configuring Firewall/VPN 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 security device to bind the VPN tunnel to the tunnel interface. The security device routes all VPN traffic through the tunnel interface to the protected resources.
Tunnel Zone—Select a pre-configured tunnel zone on the security device to bind the VPN tunnel directly to the tunnel zone. The tunnel zone must include one or more numbered tunnel interfaces; when the security device routes VPN traffic to the tunnel zone, the traffic uses one or more of the tunnel interfaces to reach the protected resources.

Monitor

You can enable VPN Monitor and configure the monitoring parameters for the device. Monitoring is off by default. To enable the VPN Monitor in Realtime Monitor to display statistics for the VPN tunnel, configure the following:

- **VPN Monitor**—When enabled, the device sends ICMP echo requests (pings) through the tunnel at specified intervals (configurable in seconds) to monitor network connectivity (the device uses the IP address of the local outgoing interface as the source address and the IP address of the remote gateway as the destination address). If the ping activity indicates that the VPN monitoring status has changed, the device triggers an SNMP trap; VPN Monitor (in RealTime Monitor) tracks these SNMP statistics for VPN traffic in the tunnel and displays the tunnel status.

- **Rekey**—When enabled, the device regenerates the IKE key after a failed VPN tunnel attempts to re-establish itself. When disabled, the device monitors the tunnel only when the VPN passes user-generated traffic (instead of using device-generated ICMP echo requests). Use the rekey option to:
  - Keep the VPN tunnel up even when traffic is not passing through.
  - Monitor devices at the remote site.
  - Enable dynamic routing protocols to learn routes at a remote site and transmit messages through the tunnel.
  - Automatically populate the next-hop tunnel binding table (NHTB table) and the route table when multiple VPN tunnels are bound to a single tunnel interface.

- **Optimized**—(This option appears only for devices running ScreenOS 5.x.) When enabled, the device optimizes its VPN monitoring behavior as follows:
  - Considers incoming traffic in the VPN tunnel as ICMP echo replies. This reduces false alarms that might occur when traffic through the tunnel is heavy and the echo replies cannot get through.
  - Suppresses VPN monitoring pings when the tunnel passes both incoming and outgoing traffic. This can help reduce network traffic.

- **Source Interface and Destination IP**—Configure these options to use VPN Monitoring when the other end of the VPN tunnel is not a security device. Specify the source and destination IP addresses.

Adding a VPN Rule

After you have configured the VPN on each device you want to include in the VPN, you can add a VPN rule to a Security Policy:
For policy-based VPNs, you must add a VPN rule to create the VPN tunnel.

For route-based VPNs, the VPN tunnel is already in place. However, you might want to add a VPN rule to control traffic through the tunnel.

For details on adding and configuring a VPN rule in a Security Policy, see “Adding VPN Rules” on page 488.

Creating L2TP VPNs

Creating device-level L2TP VPN is a three stage process:

1. Add L2TP Users
2. Configure L2TP Settings
3. Add VPN rules to Security Policy

Adding L2TP Users

For VPNs that use L2TP to provide remote access services, you must add an L2TP User to the security device. An L2TP User has an account on the security device that guards the protected resources in the VPN; when the user attempts to connect to a protected resource, the security device authenticates the user.

To add a L2TP User for a security device, in the security device configuration L2TP/XAuth/Local User, click the Add icon. Enter a name for the user, then specify:

- **User**—Select a preconfigured Local User object that is configured for L2TP.
- **Remote Setting**—Select a preconfigured Remote Settings object.
- **IP Pool**—Select a preconfigured IP Pool object.
- **Static IP**—Enter the static IP address of the Local User.

Configuring L2TP

To connect to an L2TP VPN tunnel, the L2TP RAS user uses the IP address and WINS/DNS information assigned by the user’s ISP. However, when the L2TP RAS user sends VPN traffic through the tunnel, the security device assigns a new IP address and WINS/DNS information that enables the traffic to reach the destination network.

Enter a name for the L2TP VPN, then specify the following information:

- **Host Name**—Enter the name of the L2TP host.
- **Outgoing Interface**—The outgoing interface is the interface on the security device that sends and receives VPN traffic. Typically, the outgoing interface is in the untrust zone.
- **Keep Alive**—The number of seconds a VPN member waits between sending hello packets to an L2TP RAS user.
Peer IP—Enter the IP address of the L2TP peer.

Secret—Enter the shared secret that authenticates communication in the L2TP tunnel.

Remote Settings—Select the preconfigured remote settings object that represents the DNS and WINS servers assigned to L2TP RAS users after they have connected to the tunnel.

IP Pool Name—Select the preconfigured IP pool object that represents the available IP addresses that can be assigned to L2TP RAS users after they have connected to the tunnel.

Auth Server

- Use the default settings to use the default authentication server for the domain. To change or assign a domain authentication server, edit the domain settings; for details, see “Creating Subdomains” on page 71.

- Use custom settings to specify a preconfigured authentication server object to assign TCP/IP settings to the gateway and authenticate specific L2TP User or User Groups.

Adding a VPN Rule

After you have configured the VPN on each device you want to include in the VPN, you can add a VPN rule to a Security Policy:

- For policy-based VPNs, you must add a VPN rule to create the VPN tunnel.

- For route-based VPNs, the VPN tunnel is already in place. However, you might want to add a VPN rule to control traffic through the tunnel.

For details on adding VPN rules to a Security Policy, see “Adding VPN Rules” on page 488.

Creating L2TP Over Autokey IKE VPNs

Creating a device-level L2TP-over-Autokey IKE VPN is a multi-stage process:

1. Add L2TP Users (see “Adding L2TP Users” on page 486)
2. Configure L2TP Settings (see “Configuring L2TP” on page 486)
3. Configure Peer Gateway (see “Configuring Gateways” on page 475)
4. Configure Routes (Route-based only) (see “Configuring Routes (Route-based only)” on page 479)
5. Add VPN to Device (see “Configuring the VPN” on page 480)
6. Add VPN rules to Security Policy (see “Adding a VPN Rule” on page 487)
Adding VPN Rules

To create a policy-based VPN or to add access policies to a route-based VPNs, you must add a VPN rule to a Security Policy for each device in the VPN.

Adding a VPN Rule is a three stage process:

1. Configuring the VPN rule
2. Configure Security Policy
3. Installing the Security Policy

Configuring the VPN

In Security Policies, select a predefined Security Policy (or create a new policy), and add a VPN rule. right-click in the Source Address, Destination Address, Action, or Install On column and select Configure VPN to display the Configure VPN dialog box.

- Select the source security device that contains the termination interface for the VPN tunnel.
- Select a VPN Type:
  - For IKE VPNs, select the VPN that you configured on the device.
  - For L2TP VPNs, you must also select the L2TP tunnel that you configured on the device.
- Select the Protected Resources for the VPN:
  - If both VPN termination points are security devices, choose the protected resources that represent the network components you want to protect. You can also select a predefined Global MIP or VIP for the device.
  - If the source VPN termination point is a RAS user, select Source is Dialup and choose the Protected Resources behind the destination VPN termination point that represent the network components you want to protect on the remote network.
  - If the destination VPN termination point is a RAS user, select Destination is Dialup and choose the Protected Resources behind the source VPN termination point that represent the network components you want to protect on the local network.

Configuring the Security Policy

To configure the remaining columns for the VPN rule:

- From Zone—Select the zone on the source VPN member that contains the termination interface for the VPN tunnel.
- To Zone—Select the zone on the destination VPN member that contains the termination interface for the VPN tunnel.
Service column—Select the services you want to permit in the VPN tunnel.

You do not need to configure the action—NetScreen-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 “Configuring Firewall Rule Options” on page 335.

To deny a host, use a deny rule before the VPN rule.

Assign and Install the Security Policy
You must assign the Security Policy to the each VPN member and install the Security Policy on those devices before the VPN is active.

Device-Level VPN Examples
This section provides examples of the two device-level VPN types:

- Configuring a Route-Based Site-to-Site VPN, Manual Key
- Configuring a Policy-Based Site-to-Site VPN, Manual Key
- Configuring a Policy-Based RAS VPN, L2TP

The following sections provide step-by-step instructions on creating each type of device-level VPN.

NOTE: For examples on creating other VPN types using VPN Manager, see “VPN Manager Examples” on page 452.

EXAMPLE: CONFIGURING A ROUTE-BASED SITE-TO-SITE VPN, MANUAL KEY
In this example, a Manual Key tunnel provides a secure communication channel between offices in Tokyo and Paris. The Trust zones at each site are in NAT mode. The Trust and Untrust security zones are in the trust-vr routing domain, and the Untrust zone interface (ethernet3) serves as the outgoing interface for the VPN tunnel.

To set up the tunnel, you must configure the security devices at both ends of the tunnel. First, you create the VPN components that you use to build the VPN, such as the security devices and the shared Address Objects. Next, you create the tunnel interfaces for each device and configure the VPN tunnel. You must also add the necessary static routes on each device to create the VPN tunnel. Finally, you create firewall rules in a Security Policy to control VPN traffic between the two sites.
Figure 148: RB Site-to-Site VPN, MK Example Overview

1. Add the Tokyo and Paris security devices (for details on adding devices, see Chapter 4, “Adding Devices”):

   a. Configure the Tokyo device with the following interfaces:
      - Ethernet1 is the Trust IP (10.1.1.1/24) in the Trust zone.
      - Ethernet3 is the Untrust IP (1.1.1.1/24) in the Untrust zone.

   b. Configure the Paris device with the following interfaces:
      - Ethernet1 is the Trust IP (10.2.2.1/24) in the Trust zone.
      - Ethernet3 is the Untrust IP (2.2.2.2/24) in the Untrust zone.

2. Create the Address Objects that you use in the VPN rule in the firewall rulebase (for details on creating VPN rules, see “Adding VPN Rules” on page 488).

   a. Add the Tokyo Trust LAN (10.1.1.0/24) as a network Address Object. In Address Objects, click the Add icon and select Network. Configure the following, then click OK:
      - For Name, enter Tokyo Trust LAN.
      - For IP Address/Netmask, enter 10.1.1.0/24.
      - For Color, select magenta.
      - For Comment, enter Tokyo Trust Zone.

   b. Add the Paris Trust LAN (10.2.2.0/24) as a network Address Object. In Address Objects, click the Add icon and select Network. Configure the following, then click OK:
      - For Name, enter Paris Trust LAN.
      - For IP Address/Netmask, enter 10.2.2.0/24.
3. Configure the Tokyo tunnel interface:
   a. In the navigation tree, select Device Manager > Security Devices, then
to open the device configuration.
   b. In the device navigation tree, select Network > Interface. Click the Add
icon and select Tunnel Interface. The General Properties screen for tunnel.1
appears.
   c. Configure the following, then click OK:
      - For Zone, select untrust.
      - For IP Options, select Unnumbered.
      - For Source Interface, select ethernet3.

4. Create the Tokyo VPN:
   a. In the device navigation tree, select VPN Settings > AutoKey IKE/Manual
VPN.
   b. Select the Manual tab, then click the Add icon. The Properties screen
appears. Configure the Properties tab as shown below:
      - For Name, enter Tokyo_Paris.
      - For Gateway, enter 2.2.2.2.
      - For Local IP, enter 3020.
      - For Remote SPI, enter 3030.
      - For Outgoing Interface, select ethernet3.
      - For ESP/AH, select ESP CBC.
      - For Encryption Algorithm, select 3DES-CBC.
      - Select Generate Key by Password, then enter the password
asdlk24234.
      - For Authentication Algorithm, select SHA-1.
      - Select Generate Key by Password, then enter the password PNas134a.
   c. Select the Binding tab. Enable Tunnel Interface, then select tunnel.1.
   d. Click OK to save the new VPN.
5. Create Tokyo Routes:
   a. In the device navigation tree, select Network > Virtual Router to display the list of virtual routers on the device. Double-click the trust-vr route to open the vr for editing.
   b. In the virtual router dialog box, click Routing Table, then click the add icon under destination-based Routing Table to add a new static route.
   c. Configure a route from the untrust interface to the gateway, as shown below, then click OK:

   ![Figure 149: Configure Tokyo Route for RB Site-to-Site VPN, MK](image)

   d. Configure route from the trust zone to the tunnel interface, as shown below, then click OK:
Device-Level VPN Examples

Figure 150: Configure Tokyo Trust Route for RB Site-to-Site VPN, MK

Your routing table should appear as shown below:

Figure 151: View Tokyo Routing Table for RB Site-to-Site VPN, MK

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Mask</th>
<th>Next Hop</th>
<th>Interface</th>
<th>Vsys</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>0</td>
<td></td>
<td>ethernet3</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Gateway IP Address: 1.1.1.250</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Metric: 1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Tag:</td>
<td></td>
</tr>
<tr>
<td>10.2.2.0</td>
<td>24</td>
<td></td>
<td>tunnel.1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Gateway IP Address: 0.0.0.0</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Metric: 1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Tag:</td>
<td></td>
</tr>
</tbody>
</table>

e. Click OK to save your changes to the virtual router, then click OK to save your changes to the Tokyo device.

6. Configure the Paris Tunnel Interface:

a. In Device Manager, double-click the device icon for Paris to open the device configuration.

b. In the device navigation tree, select Network > Interface. Click the Add icon and select Tunnel Interface. The General Properties screen appears.

c. Configure the following, then click OK:

   - For Zone, select untrust.
7. Create the Paris VPN:

a. In the device navigation tree, select VPN Settings > AutoKey IKE/Manual VPN.

b. Select the Manual tab, then click the Add icon. The Properties screen appears.

c. Configure the following:

- For Name, enter Paris_Tokyo.
- For Gateway, enter 2.2.2.2.
- For Local SPI, enter 3020.
- For Remote SPI, enter 3030.
- For Outgoing Interface, select ethernet3.
- For ESP/AH, select ESP CBC.
- For Encryption Algorithm, select 3DES-CBC, then select Generate Key by Password and enter the password asdlk24234.
- For Authentication Algorithm, select SHA-1, then select Generate Key by Password and enter the password PNas134a.

d. Select the Binding tab. Enable Tunnel Interface, then select tunnel.1.

e. Click OK to save the new VPN.


a. In the device navigation tree, select Network > Virtual Router to display the list of virtual routers on the device.

b. Double-click the trust-vr route to open the vr for editing.

c. In the virtual router dialog box, click Routing Table, then click the add icon under destination-based Routing Table to add a new static route.

d. Configure a route from the untrust interface to the gateway, as shown below, then click OK:

NOTE: ScreenOS 4.0.x devices display only the destination-based Routing Table; ScreenOS 5.0.x devices display both destination-based and source-based routing tables; ScreenOS 5.1 and higher devices display destination-based, source-based, and source interface-based routing tables.
Figure 152: Configure Paris Untrust Route for RB Site-to-Site VPN, MK

Your routing table should appear as shown below:

Figure 153: Configure Paris Trust Route for RB Site-to-Site VPN, MK

Your routing table should appear as shown below:
Device-Level VPN Examples

9. Create the Security Policy:

a. In the main navigation tree, select Security Policies. Click the Add icon to display the New Security Policy dialog box.

b. Configure the following, then click OK:
   - For Security Policy Name, enter Corporate Route-based VPNs.
   - Add comments, if desired.

c. In the main navigation tree, select Security Policies > Corporate Route-based VPNs. The security policy appears in the main display area. Configure the rules as shown below:

EXAMPLE: CONFIGURING A POLICY-BASED SITE-TO-SITE VPN, MANUAL KEY

In this example, a Manual Key tunnel provides a secure communication channel between offices in Tokyo and Paris, using ESP with 3DES encryption and SHA-1 authentication. The Trust zones at each site are in NAT mode. The Trust and Untrust security zones and the Untrust-Tun tunnel zones are in the trust-vr routing domain. The Untrust zone interface (ethernet3) serves as the outgoing interface for the VPN tunnel.
To set up the tunnel, you must configure the security devices at both ends of the tunnel. First, you create the VPN components that you use to build the VPN, such as the security devices and the shared Address Objects. Next, you configure the VPN tunnel and add the necessary static routes on each device. Finally, you create VPN rules in a Security Policy to create the VPN tunnel between the two sites.

Figure 156: PB Site-to-Site VPN, MK Example Overview

1. Create VPN Components:
   - Security Devices. See “Add the Tokyo and Paris security devices (for details on adding devices, see Chapter 4, “Adding Devices”):” on page 490.
   - Address Objects. See “Create the Address Objects that you use in the VPN rule in the firewall rulebase (for details on creating VPN rules, see “Adding VPN Rules” on page 488).” on page 490.

2. Create the Tokyo VPN:
   a. In the device navigation tree, select VPN Settings > AutoKey IKE/Manual VPN.
   b. Select the Manual tab, then click the Add icon. The Properties screen appears. Configure the following:
      - For Name, enter Tokyo_Paris.
      - For Gateway, enter 2.2.2.2.
      - For Local SPI, enter 3020.
      - For Remote SPI, enter 3030.
      - For Outgoing Interface, select ethernet3.
      - For ESP/AH, select ESP CBC.
      - For Encryption Algorithm, select 3DES-CBC.
Device-Level VPN Examples

Select Generate Key by Password, then enter the password asdk24234.

For Authentication Algorithm, select SHA-1.

Select Generate Key by Password, then enter the password PNas134a.

c. Select the Binding tab. Enable Tunnel Zone and select untrust-tun.

d. Click OK to save the new VPN.


4. Create the Paris VPN:
   a. In the device navigation tree, select VPN Settings > AutoKey IKE/Manual VPN.

   b. Select the Manual tab, then click the Add icon. The Properties screen appears.

   c. Configure the following:

      i. For Name, enter Paris_Tokyo.

      ii. For Gateway, enter 2.2.2.2.

      iii. For Local SP, enter 3020.

      iv. For Remote SPI, enter 3030.

      v. For Outgoing Interface, select ethernet3.

      vi. For ESP/AH, select ESP CBC.

      vii. For Encryption Algorithm, select 3DES-CBC, then select Generate Key by Password and enter the password asdk24234.

      viii. For Authentication Algorithm, select SHA-1, then select Generate Key by Password and enter the password PNas134a.

   d. Select the Binding tab. Enable Tunnel Zone and select untrust-tun.

   e. Click OK to save the new VPN.


6. Create the Security Policy:
   a. In the main navigation tree, select Security Policies. Click the Add icon to display the new Security Policy dialog box.

   b. Configure the following, then click OK:

      i. For Security Policy Name, enter Corporate Policy-Based VPN.
- Enter comments, if desired.

c. In the main navigation tree, select Security Policies > Corporate Policy-Based VPN. The security policy appears in the main display area. Configure two VPN rules as shown below:

Figure 157: Configure Two VPN Rules for PB Site-to-Site VPN, MK

<table>
<thead>
<tr>
<th>No.</th>
<th>From Zone</th>
<th>Source</th>
<th>To Zone</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>trust</td>
<td>Tokyo Trust LAN</td>
<td>untrust</td>
<td>Paris Trust LAN</td>
<td>ANY any</td>
<td>tunnel</td>
<td>Tokyo</td>
</tr>
<tr>
<td>2</td>
<td>trust</td>
<td>Paris Trust LAN</td>
<td>untrust</td>
<td>Tokyo Trust LAN</td>
<td>ANY any</td>
<td>tunnel</td>
<td>Paris</td>
</tr>
</tbody>
</table>

- Rule 1 creates the VPN tunnel from the Tokyo device to the Paris device.
- Rule 2 creates the VPN tunnel from the Paris device to the Tokyo device.

d. Save the Security Policy.
EXAMPLE: CONFIGURING A POLICY-BASED RAS VPN, L2TP
In this example, you create a RAS user group called Field Sales and configure an L2TP tunnel called Sales_Corp, using ethernet3 (Untrust zone) as the outgoing interface for the L2TP tunnel. The security device applies the default L2TP tunnel settings to the RAS user group.

NOTE: An L2TP-only configuration is insecure and is recommended only for debugging.

The remote L2TP clients are on Windows 2000 operating systems. For information on how to configure L2TP on the remote clients, refer to Windows 2000 documentation. Only the configuration for the security device end of the L2TP tunnel is provided below.

Figure 158: PB RAS VPN, L2TP Example Overview

1. Configure the L2TP user objects:
   a. Configure an L2TP user object for Adam, then click OK:
      - For Name, enter Adam.
      - Select Enable, then select L2TP.
      - Select Password, then enter and confirm the password: AJbioJ15.
   b. Configure an L2TP user object for Betty, then click OK:
      - For Name, enter Betty.
      - Select Enable, then select L2TP.
      - Select Password, then enter and confirm the password: BviPsoj1.
   c. Configure an L2TP user object for Carol, then click OK:
      - For Name, enter Carol.
      - Select Enable, then select L2TP.
      - Select Password, then enter and confirm the password: Cs10kdD3.
2. Create a local user group called Field Sales that includes the Adam, Betty, and Carol local user objects. For details on creating a local user group, see “Configuring User Objects” on page 298.

3. Configure the Remote Settings object. Configure the following, then click OK:
   - For Name, enter RM_L2TP.
   - For Color, select green.
   - For Dns1, enter 1.1.1.2.
   - For Dns2, enter 1.1.1.3.
   - For Wins1, enter 0.0.0.0.
   - For Wins2, enter 0.0.0.0.
   For details on creating Remote Settings objects, see “Configuring Remote Settings” on page 307.

4. Configure the IP Pool object. Configure the following, then click OK:
   - For IP Pool Name, enter Global.
   - For Color, select magenta.
   - For Start IP, enter 10.10.2.100.
   - For End IP, enter 10.10.2.180.
   For details on creating IP Pool objects, see “Configuring IP Pools” on page 303.

5. Configure the L2TP tunnel:
   a. In Device Manager, double-click the device icon for the device on which you want to configure the L2TP tunnel.
   b. In the device navigation tree, select VPN Settings > L2TP. In the main display area, click the Add icon. The null-L2TP tunnel dialog box appears.
   c. Configure the following, then click OK:
      - For Name, enter Sales_Corp.
      - For Outgoing Interface, select ethernet3.
      - For Keep Alive, enter 60.
      - For Peer IP, enter 0.0.0.0 (because the peer’s ISP dynamically assigns it an IP address, enter 0.0.0.0 here).
      - Select Use Custom Settings, and leave the default authentication server as Local.
      - For User/Group, select Dialup Group, then select Field Sales.
d. Click OK to save your changes to the device.

6. Configure a rule in the Zone Rulebase of a Security Policy, as shown below:

Figure 159: Configure Rule for PB RAS VPN, L2TP

<table>
<thead>
<tr>
<th>No.</th>
<th>Match</th>
<th>Action</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>![Match Diagram]</td>
<td>![Action Diagram]</td>
<td>![Install Diagram]</td>
</tr>
</tbody>
</table>

![Configure VPN Diagram]
Chapter 11
Central Manager

Central Manager provides super admins with the opportunity to manage up to ten concurrent regional servers from the NetScreen-Security Manager (NSM) management system. With Central Manager, you can log into the system and perform operations such as enforcing global policies, adding regional servers, adding, modifying, and deleting pre/post rules and shared objects, and managing polymorphic objects.

NOTE: In 2007.2 NSM, Central Manager runs exclusively on NSMXpress.

This chapter contains the following sections:

- Central Manager Overview on page 504
- Installing Global Policy to a Regional Server on page 510
Central Manager Overview

Predefined shared objects are shared by Central Manager and regional servers. Any predefined shared objects used by Central Manager pre/post rules are available in regional servers, specifically, attack db and etc. When updating pre/post rules, the version of Central Manager and regional server must match.

Figure 160: Central Manager UI and Regional Server UI
Regional Server and Central Manager Self-Sufficiency

Both the Central Manager and the regional servers are self-sufficient and independent from the other being online.

Self-Sufficient Central Manager

Central Manager is independent of the regional servers and can run without any regional server online. The Central Manager admin can add, modify, or delete pre/post rules and shared objects. Data is not lost when logging on and off of Central Manager. In addition, Central Manager does not use any of the shared objects that exist only in any of the individual regional servers.

Self-Sufficient Regional Server

Regional servers can enforce global policies even when Central Manager is not running. Regional servers maintain copies of pushed Central Manager pre/post rules and associated objects. In addition, regional servers do not use any Central Manager data directly.

Super Admin User

The Central Manager super admin accounts have access to all features offered in Central Manager. The super user is created while installing Central Manager. It is also the only admin account created during installation.

As a super admin user, you can use the single sign-on feature (see Figure 161 below) to access regional servers directly from Central Manager without logging out of Central Manager inputting regional server login credentials.

Figure 161: Single Sign-On

Regional Server Management

Central Manager treats regional servers as objects similar to other objects. As with other objects, Central Manager can add, modify, and delete regional servers. Regional server objects are shared objects that contain essential connection information such as its own IP address, port, and so on. Central Manager admins can use additional credential information in the regional server objects to sign onto each regional server.
Once logged into a Central Manager server, super admins can select any of the regional servers managed by Central Manager and begin managing the servers using all assigned permissions. No extra log on/off steps are required for admins to navigate from one regional server to another or from Central Manager server to a regional server. Any regional server accessible through Central Manager, is opened using a separate window. There is a maximum number of 25 concurrent regional servers Central Manager can open at any one time.

Using Central Manager

This section provides procedures for the following tasks for Central Manager super users:

- Adding a Regional Server Object
- Deleting a Regional Server Object
- Logging into a Regional Server

Adding a Regional Server Object

For a Central Manager admin to log onto a regional server, one of the regional server admin credentials must be used and linked to the Central Manager admin.

The following procedure assumes that a Central Manager admin is logged onto a Central Manager client.

To add a regional server object:

1. In the main navigation tree, select **Object Manager > Regional Server**.

2. Click the Add icon in the toolbar.

3. Enter the following information for the regional server you want to add.
   - Name
   - IP address
   - Backup IP address (optional)
4. Click the Add icon in the admin table to add regional server admin(s).

5. Enter the following information for the regional server you want to add.
   - Admin name
   - Admin password

6. Click the Add icon in the admin table to link the newly created regional server object to the Central Manager admin.

7. Select a Central Manager admin from the drop down list box.
8. Click OK in all the open boxes to save the options and close each window.

Deleting a Regional Server Object

The following procedure assumes that a Central Manager admin is logged onto a Central Manager client and a regional server object has been created.

To delete a regional server object:

1. In the main navigation tree, select Object Manager > Regional Server.
2. Right-click the regional server you want to delete.

Figure 166: Deleting a Regional Server Object

3. In the Delete Regional Server dialog box, click Next to delete the object.

Logging into a Regional Server

Central Manager admins can log into regional servers directly from Central Manager.

The following procedure assumes that a Central Manager admin is logged onto a Central Manager client and a regional server object has been created.
To switch from Central Manager to a regional server:

1. In the toolbar, click the **Login to Regional Server** drop down list.

Figure 167: Log into a Regional Server

2. Select a regional server to open to launch the selected regional server in a separate window (see Figure 168 below).

Only a Central Manager admin can log into any other regional servers. A regional server admin cannot log into another regional server or a central manager server.
Installing Global Policy to a Regional Server

During the Global Policy Install on the Central Manager server, all pre/post rules as well as the global polymorphic and shared objects on the Central Manager server are updated to regional servers managed by Central Manager. The Central Manager admin can select which regional servers will receive the Central Manager rules and objects during the install.
Pre/Post Rules update during Global Policy Install

Pre/post rules exist on the Central Manager server under a separate policy object in the Policy Manager. When updating to the regional server during the Global Policy Install these rules are created in the regional server under a new global policy in the global domain. All global policies existing on the regional server prior to the Global Policy Install are removed, and replaced completely with the new global policies from Central Manager. Only those global rules which have the regional server object included in the Install On column, as well as rules with the Any entry in the Install On column, will be updated to that regional server.

Global Policy Install is a directive that is dispatched as a job with many tasks. Each task represents an install operation to a specific server. Job manager reports the status of each task. Each task is executed independently of other task’s status. If one task fails, as well as “Job Manager entries, this failure does not prevent another task from finishing successfully. Audit log entries are generated on both the Central Manager and regional servers.

Shared Objects Update During Global Policy Install

All shared objects (both polymorphic and regular) existing on the Central Manager server are updated to regional servers during the Global Policy Install if they are referenced in a pre/post rule. Note that objects are updated only if they are actually being used by the pre/post rules on the Central Manager server. All new shared objects are replicated/inserted into the global domain of the regional server. Objects that are not used are not updated.

Name Space Conflict Resolution for Shared Objects

When a regular shared object is replicated to a regional server during the Global Policy Install, the following name conflict scenarios could occur:

- **Conflict with a regional server shared object of the same name and same type content**—Existing shared objects will be kept and the incoming shared object will be discarded. The incoming global policy rules use the existing shared object.

- **Conflict with a regional server shared object of the same name, but different content**—An attempt is made to match the content of an incoming shared object with another shared object named “objname_n” where “n” is a sequentially increasing integer. The incoming global policy rules use the newly created shared object.

- **Conflict with the previously replicated polymorphic object of the same type**—The incoming shared object is renamed “objname_n” where “n” is a sequentially increasing integer and is inserted into the regional server’s global domain.

Since polymorphic objects cannot be deleted by the regional server administrator, some of the polymorphic objects that exist in the global domain of the regional server are deleted as a first step in the Global Policy Install transaction.

All polymorphic objects are deleted if they are not used by any of the local policies in the regional server.
Name Space Conflict Resolution for Polymorphic Objects

When a polymorphic object is replicated to a regional server during the Global Policy Install, the following name conflict scenarios could occur:

- **Name conflict with a previously replicated polymorphic object**—To keep the customization information the regional server admin added, existing polymorphic object are kept, and incoming global policy rules use existing polymorphic object. Incoming polymorphic object with the same name are discarded.

- **Name conflict with a regional server regular shared object of the same type**—The incoming polymorphic object is renamed “objname_n” where “n” is a sequentially increasing integer and inserted into the regional server’s global domain.

---

**NOTE:** Only names are pushed for polymorphic objects.
Part 4
Monitoring

The chapters in Part 4 of the NetScreen-Security Manager Administrators Guide are designed to help you monitor the status of your security devices (and VPN tunnels), as well as use log entries and reports to review and ensure the efficiency of your Security Policies.

Part 4 contains the following chapters:

- Chapter 12 “Realtime Monitoring” details the firewall, VPN, and NSRP monitoring functionality of NetScreen-Security Manager.

- Chapter 13 “Analyzing Your Network” details the Profiler, a network-analysis tool that helps you learn about your internal network, enabling you to create effective Security Policies and minimize unnecessary log records.

- Chapter 14 “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 15 “Reporting” details how to create reports from log information.

For additional information about specific terms, objects, or functionality referred to in this guide, see Part 5, “Appendixes” on page 673. For help in locating documentation for a term, task, or concept in this guide, see Part 6, “Index” on page 779.
Chapter 12
Realtime Monitoring

This chapter describes how to use the Realtime Monitor module in Juniper Networks NetScreen-Security Manager to monitor the status and traffic statistics for all the managed Juniper Networks security devices in your network in real time. You can use the Realtime Monitor to monitor and track the day-to-day health and performance of your network security devices, VPN tunnels, and NSRP clusters.

It also describes how to use the Server Manager module to monitor the status of the NetScreen-Security Manager management system.

This chapter contains the following sections:

- About the Realtime Monitor on page 516
- Monitoring Security Devices on page 517
- Monitoring IDP Sensors on page 541
- Monitoring VPNs on page 545
- Monitoring NSRP Statistics on page 547
- Monitoring IDP Clusters on page 549
- Using The Realtime Monitor on page 551
- Monitoring the Management System on page 552
About the Realtime Monitor

The Realtime Monitor module in NetScreen-Security Manager enables you to monitor real time status and statistics about all the managed security devices, VPN tunnels, NSRP clusters, IDP sensors and IDP clusters in your network at a glance. You can use the Realtime Monitor to identify problems, track security events, and discover trends across multiple geographic regions and functional areas from a central management location.

The Realtime Monitor can also help you quickly identify potential device, network, or even system-level problems, such as:

- Configuration status—At the device level, you can monitor the changing status of one or more security devices in real time.
- Connection Status—At the network level, you can monitor problems that could lead to failed devices.
- Performance—At the system level, you can monitor the activity between VPN members or NSRP cluster.

The Realtime Monitor tracks the integrity of your security perimeter by continually monitoring your security devices for security events (failed security devices, abnormal utilization, general errors). The Realtime monitor does the work of a management expert by first gathering information about specific processes and network activity, then color-coding each event to organize problems.

NOTE: If you previously implemented historical reporting in Juniper Networks Global PRO, and you want to continue generating statistical reports based on historical information, it is highly recommended that you install NetScreen-Statistical Report Server. If you choose not to install NetScreen-Statistical Report Server, you can still continue to use historical reports with NetScreen-Security Manager to track Service Level Agreement, traffic, and resource statistics on security devices running ScreenOS 4.0.x. Refer to the NetScreen-Security Manager 2004 FP2 Migration Guide for more information.

Realtime Monitor Views

The Realtime Monitor includes four views:

- Device Monitor—Displays status information on the managed security devices in your network. This includes the name and type of the device managed in NetScreen-Security Manager, connection status, and current configuration status. From the Device Monitor, you can also access more detailed information and statistics on each security device including ScreenOS, mode, CPU utilization, memory, sessions, and network traffic. You can also use the Device Monitor to view status information on IDP sensors managed in your network.

- 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.
Monitoring Security Devices

Use the Device Monitor to get an at-a-glance view of the current status of all the managed security devices and IDP sensors in your network.

If you have configured multiple sub-domains, you can view all your managed devices from the global domain.

Information provided by the Device Monitor includes:

- Up/down connection status
- Configuration status
- Name, type and firmware version running

Figure 169: Device Monitor Dialog Box

Viewing Device Status

The following table lists and describes device information that you can view through the Device Monitor:
Table 33: Device Status Information

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name assigned to the device in NetScreen-Security Manager</td>
</tr>
<tr>
<td>Domain</td>
<td>Domain in NetScreen-Security Manager in which the device is managed. Note: If you have configured multiple sub-domains, you can view all your managed devices from the global domain.</td>
</tr>
<tr>
<td>Device Type</td>
<td>Model number of the device.</td>
</tr>
<tr>
<td>Managed OS Version</td>
<td>ScreenOS firmware version running on the device.</td>
</tr>
<tr>
<td>Config Status</td>
<td>Displays the current configuration status of the device in NetScreen-Security Manager:</td>
</tr>
<tr>
<td></td>
<td>- None. No state has been set (does not show in Device Monitor).</td>
</tr>
<tr>
<td></td>
<td>- Modeled. The device exists in NetScreen-Security Manager, but a connection to the device has not yet been established.</td>
</tr>
<tr>
<td></td>
<td>- RMA. Equivalent to bringing the device into the Modeled state. RMA results from an admin selection in the User Interface when a security device goes down.</td>
</tr>
<tr>
<td></td>
<td>- Waiting for 1st connect. NetScreen-Security Manager is waiting for the device to connect. You must enter a command on the device to make it connect to NetScreen-Security Manager.</td>
</tr>
<tr>
<td></td>
<td>- Import Needed. You must import the configuration of the device into NetScreen-Security Manager. When you add a device running ScreenOS 5.x for the first time, verify that your status indicates “Import Needed” before you attempt to import the device. During migration, this state indicates that import of the security device configuration is still required.</td>
</tr>
<tr>
<td></td>
<td>- OS Version Adjustment Needed. The firmware version detected running on the device is different than what was previously detected in NetScreen-Security Manager. This could happen in the event that the automatic adjustment option was cleared during a change device firmware directive.</td>
</tr>
<tr>
<td></td>
<td>- Update Needed. An update to this device is required.</td>
</tr>
<tr>
<td></td>
<td>- Managed. The device is currently being managed by NetScreen-Security Manager.</td>
</tr>
</tbody>
</table>

For devices running ScreenOS 5.1 and higher, the Device Monitor can display the following additional configuration states:

| Managed, In Sync. | The physical device configuration is synced with the modeled configuration in NetScreen-Security Manager. |
| Managed, Device Changed. | The physical device configuration is out-of-sync with the modeled configuration in NetScreen-Security Manager. Changes were made to the physical device configuration (the configuration on the physical device is newer than the modeled configuration). |
| Managed, NSM Changed. | The modeled device configuration is out-of-sync with the physical device configuration. Changes were made to the modeled configuration (the configuration on the NetScreen-Security Manager is newer than the physical device configuration). |
| Managed, NSM and Device Changed. | Both device configurations (physical and modeled) are out-of-sync each other. Changes were made to the physical device configuration and to the modeled configuration. |
Device Polling Intervals

NetScreen-Security Manager retrieves device statistics from the physical security device. The device polling interval determines the number of seconds the Device Server waits before polling for new statistics.

To configure or view the device polling intervals, double-click the Server Manager > Servers node, then select the Device Server and click the Edit icon. Use the Device Polling tab to edit the intervals to meet your monitoring requirements:

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
<th>Poll Interval (in secs)</th>
<th>Save Interval (in secs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>Details traffic, interface, zone, and system-related statistics on a specific device. Information appears in the Device Monitor.</td>
<td>300</td>
<td>300</td>
</tr>
<tr>
<td>VPN</td>
<td>Details VPN tunnels between your managed devices, including VPN tunnel status (Up, Down, Not Monitored), VPN name, VPN Type, VPN source, VPN destination, security parameter index (SPI), IP address, and protocol. Information appears in the VPN Monitor.</td>
<td>300</td>
<td>300</td>
</tr>
</tbody>
</table>
Viewing Additional Device Detail and Statistics

If a device is up and running, you can also access additional information on the device. To view additional status, you can view Device Details. For traffic-related statistics and other information, you can View Statistics.

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
<th>Poll Interval (in secs)</th>
<th>Save Interval (in secs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>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>300</td>
<td>300</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>300</td>
<td>300</td>
</tr>
</tbody>
</table>

NOTE:  If a security device is never connected, the Device Detail Status and Statistics views for the device are not available.

Viewing Device Details

Double-click on any device to view additional details on the device related to resource usage. You can also right-click on the device and select View Details.

NOTE:  The information in the Details window appears slightly different for firewall/VPN devices and IDP sensors. Details for IDP sensors also include an additional tab enabling you to view process status.
The following table lists and describes the information that you can view for a security device through the Device Detail Status:

**Table 35: Device Detail Status Items**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS Version</td>
<td>Indicates the ScreenOS firmware version running on the device.</td>
</tr>
<tr>
<td>Mode</td>
<td>Current operation mode of the device. Network Address Translation (NAT), Transparent, or Route.</td>
</tr>
<tr>
<td>Latest Reboot</td>
<td>Indicates the most recent date and time that the security device was powered off and on. You can use this information to determine how long the security device was down.</td>
</tr>
<tr>
<td>CPU Utilization</td>
<td>The percent of the CPU being used at the moment of the status snapshot.</td>
</tr>
<tr>
<td>One Min. Load</td>
<td>The percent CPU utilization average on the security device for the last 1 min.</td>
</tr>
<tr>
<td>5 Min. Load</td>
<td>The percent CPU utilization average on the security device for the last 5 mins.</td>
</tr>
<tr>
<td>15 Min. Load</td>
<td>The percent CPU utilization average on the security device for the last 15 mins.</td>
</tr>
<tr>
<td>Mem Allocated</td>
<td>The original amount of memory allocated to the security device.</td>
</tr>
<tr>
<td>Mem Left</td>
<td>The amount of allocated memory that remains after being used by the security device.</td>
</tr>
</tbody>
</table>
Viewing Device Statistics

If a security device is up and running, you can also access the Statistics view to access traffic, interface, zone, and other system-related information on the device. To view statistics on a particular security device, right-click the security device in either the Device Monitor or the Device Manager and select View Statistics. The Device Statistics Summary appears in a new window.

NOTE: The information in the Device Statistics window appears slightly different for firewall/VPN devices and IDP sensors.

Device Statistics Summary

The Device Statistics Summary displays the following details:

- Details describing the security device or virtual system, for example, serial number and IP address, type, and firmware version.
- Interface information
- Device status
- Time-related statistics such as last connect or reboot

The following table details all the information you can view from the Device Statistics Summary.

Table 36: 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 security device.</td>
</tr>
<tr>
<td></td>
<td>Vsys: Displays the serial number of the security device.</td>
</tr>
<tr>
<td>Vsys</td>
<td>The name of the virtual system (if applicable)</td>
</tr>
<tr>
<td>Version</td>
<td>The security device’s build, model, and operation mode (this is not displayed in the Vsys view).</td>
</tr>
<tr>
<td>DC IP</td>
<td>The IP Address of the Device Server (this is not displayed in the Vsys view).</td>
</tr>
<tr>
<td>Interface Information</td>
<td>The employed interfaces. For example: Trust, Untrust, and Self.</td>
</tr>
<tr>
<td>Vsys Information</td>
<td>The virtual systems associated with this security device (this is not displayed in the Vsys view).</td>
</tr>
</tbody>
</table>
Additional Device Specific Views

From the Device Statistics Summary, you can access additional information enabling you to view and monitor key traffic, interface, zone, and other system-related information on a specific security device.

The following table describes each device-specific view.

Table 37: Device Specific Views

<table>
<thead>
<tr>
<th>Item</th>
<th>Displays</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Known Connect Time</td>
<td>The last time the security device connected to the Data Collector (this is not displayed in the Vsys view).</td>
</tr>
<tr>
<td>Device Status</td>
<td>Whether the security device is currently up or down (this is not displayed in the Vsys view)</td>
</tr>
<tr>
<td>Last Reboot Time</td>
<td>The last time the system was restarted (this is not displayed in the Vsys view).</td>
</tr>
<tr>
<td>Last Known Uptime</td>
<td>If the security device is down, the entry lists the last time it was up. Used to determine how long a security device was down (this is not displayed in the Vsys view).</td>
</tr>
<tr>
<td>GMT Time Offset (Hours)</td>
<td>The hour the security device is set from Greenwich Mean Time (this is not displayed in the Vsys view).</td>
</tr>
<tr>
<td>DayLight-Saving</td>
<td>If you have enabled the security device to adjust time for daylight savings.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Item</th>
<th>Displays</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic</td>
<td>View traffic on the security device distributed by policy. Enables you to view a chart of the traffic distribution by policy.</td>
</tr>
<tr>
<td>Protocol Distribution</td>
<td>View traffic on the security device distributed by protocol. Enables you to view a chart of the traffic distribution by protocol.</td>
</tr>
<tr>
<td>VPN Distribution</td>
<td>View the up/down status and active statistics of VPNs on the security device (if applicable). Also enables you to view a chart of the VPN distribution by VPN tunnel.</td>
</tr>
<tr>
<td>Interface</td>
<td>View security device traffic over specific interfaces. Enables you to view a chart of the utilization distributed by interface.</td>
</tr>
<tr>
<td>Flow Statistics</td>
<td>View security device traffic on flow counters over specific interfaces. Enables you to view a chart of flow statistics distributed by interface.</td>
</tr>
<tr>
<td>Attack Statistics</td>
<td>View all of the attacks that have occurred on a security device over specific interfaces. Enables you to view a chart of attacks distributed by interface.</td>
</tr>
</tbody>
</table>
Viewing Device Traffic Distribution

You can view statistics describing the traffic on a specific security device including how the traffic is distributed, by policy, protocol, or VPNs (if applicable). You can use this information to help you identify those policies, protocols and VPN tunnels that are most and least frequently being used on a security device.

Viewing Traffic Distribution by Security Policy

Click Policy Distribution to view security device traffic that matches the access policies configured for a security device. A bar graph appears (under the Chart tab) depicting the distribution of data by policy. The graph displays a percentage of the absolute number of bytes for the top 10 policies by default.

<table>
<thead>
<tr>
<th>View Type</th>
<th>View</th>
<th>Enables you to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zone</td>
<td>Ethernet Statistics</td>
<td>View security device traffic from specific zones. Enables you to view a chart of the traffic distributed by zone.</td>
</tr>
<tr>
<td></td>
<td>Flow Statistics</td>
<td>View security device traffic on flow related statistics for specific interfaces. Enables you to view a chart of flow statistics distributed by zone.</td>
</tr>
<tr>
<td></td>
<td>Attack Statistics</td>
<td>View all counters related to attacks that have occurred on a security device from specific zones. Enables you to view a chart of the attacks distributed by zone.</td>
</tr>
<tr>
<td>System</td>
<td>Resource Statistics</td>
<td>View CPU utilization and memory allocation statistics on the security device. Enables you to view CPU, Memory and Session Utilization trends.</td>
</tr>
<tr>
<td></td>
<td>Active Statistics</td>
<td>View administrator and user activities; active VPNs; and authenticated users on a security device. Also enable s you to view a snapshot of the ongoing active sessions on the security device.</td>
</tr>
<tr>
<td>HA</td>
<td>NSRP Statistics</td>
<td>View NSRP statistics related to clusters created on the security device (if applicable).</td>
</tr>
</tbody>
</table>
The following table describes all of the information that is available from the Policy Distribution view.

**Table 38: Policy Distribution Items.**

<table>
<thead>
<tr>
<th>Item</th>
<th>Displays</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy ID</td>
<td>the unique identifier of the policy.</td>
</tr>
<tr>
<td>Source IP</td>
<td>the IP address of the host generating the session.</td>
</tr>
<tr>
<td>Source IP Mask</td>
<td>the IP address mask for the host or network generating the session.</td>
</tr>
<tr>
<td>Destination IP</td>
<td>the IP address of the host receiving the session.</td>
</tr>
<tr>
<td>Destination IP Mask</td>
<td>the IP address mask for the host or network receiving the session.</td>
</tr>
<tr>
<td>Source Zone</td>
<td>Zone of the host generating the session.</td>
</tr>
<tr>
<td>Destination Zone</td>
<td>Zone of the host receiving the session.</td>
</tr>
<tr>
<td>VPN Name</td>
<td>Name of the Virtual Private Network.</td>
</tr>
<tr>
<td>Service</td>
<td>the application or service associated with the policy. Examples include Mail, FTP, SNMP, AOL, Telnet, and LDAP.</td>
</tr>
</tbody>
</table>
Adjusting Data Depicted Graphically

You can adjust all elements depicted in the graph including the policies, data values (such as absolute or delta), and type of data (bytes in or out, packets in or out, utilization).

To adjust policies depicted graphically:

1. Right-click within the chart and select Configure Policies. A dialog enabling you to select which policies to view appears.
2. Clear the Default checkbox.
3. Click to select the policies that you wish to view on the graph from the list of Available Policies. Click Add to add the policies that you want to the list of Selected Policies.
4. Click to select the policies that you no longer wish to view on the graph from the list of Selected Policies. Click Remove to remove the policies from the list of Selected Policies.
5. Click OK to apply your changes; or click Cancel to cancel your changes.

To adjust data and data types depicted graphically:

1. Right-click the Chart view.
2. From the Data option, select either Delta or Absolute.
3. From the Data Type option, select either Connections, Bytes, or Packets.
4. Click OK to apply your changes; or click Cancel to cancel your changes.

<table>
<thead>
<tr>
<th>Item</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>the activity to be performed, such as Permit, Deny, or Tunnel.</td>
</tr>
<tr>
<td>Total Connections</td>
<td>the total number of data connections.</td>
</tr>
<tr>
<td>Connection Rel%</td>
<td>the relative percentage of connections.</td>
</tr>
<tr>
<td>Delta Connection</td>
<td>the total numerical difference between the current connection value and the previous connection value.</td>
</tr>
<tr>
<td>Total Bytes</td>
<td>the total number of data bytes.</td>
</tr>
<tr>
<td>Bytes Rel%</td>
<td>the relative percentage of bytes.</td>
</tr>
<tr>
<td>Delta Bytes</td>
<td>the total numerical difference between the current bytes value and the previous bytes value.</td>
</tr>
<tr>
<td>Total Packets</td>
<td>the total number of data packets.</td>
</tr>
<tr>
<td>Packets Rel%</td>
<td>the relative percentage of packets.</td>
</tr>
<tr>
<td>Delta Packets</td>
<td>the total numerical difference between the current bytes value and the previous packets value.</td>
</tr>
<tr>
<td>Policy Name</td>
<td>name of the policy.</td>
</tr>
</tbody>
</table>
**Viewing Traffic Distribution by Protocol**

click the Protocol Distribution node to view the distribution of traffic according to the protocols flowing through the device. Protocols are predefined services (such as, HTTP, SNMP, or Telnet) that are enabled for each security device. You can view up to ten protocols. A bar graph appears similar to the one presented for viewing traffic according to policy distribution. The graph displays a percentage of the absolute number of bytes for the top 10 protocols by default.

**Figure 172: Protocol Distribution Dialog Box**

The following table describes all of the information that is available from the Protocol Distribution view:

<table>
<thead>
<tr>
<th>Item</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>the name of the predefined service (like HTTP, SNMP, or Telnet) operating on the selected interface.</td>
</tr>
<tr>
<td>Interface</td>
<td>the type of interface through which the protocol is flowing.</td>
</tr>
<tr>
<td>Bytes In</td>
<td>the number of incoming bytes for the protocol through the security device.</td>
</tr>
</tbody>
</table>
Adjusting Data Depicted Graphically

You can adjust the interfaces (such as Trust, Untrust, Management, NSRP, and Self) and data depicted graphically in the same way that you adjust the Policy Distribution graphs.

<table>
<thead>
<tr>
<th>Item</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bytes In Rel%</td>
<td>Relative percentage of all incoming bytes.</td>
</tr>
<tr>
<td>Delta Bytes In</td>
<td>the total numerical difference between the current bytes in value and the</td>
</tr>
<tr>
<td></td>
<td>previous bytes in value.</td>
</tr>
<tr>
<td>Bytes Out</td>
<td>the number of outgoing bytes for the protocol through the security device.</td>
</tr>
<tr>
<td>Bytes Out Rel%</td>
<td>Relative percentage of all outgoing bytes.</td>
</tr>
<tr>
<td>Delta Bytes Out</td>
<td>the total numerical difference between the current bytes out value and the</td>
</tr>
<tr>
<td></td>
<td>previous bytes out value.</td>
</tr>
<tr>
<td>Packets In</td>
<td>the number of incoming packets handled by the protocol through the security</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>previous packets in value.</td>
</tr>
<tr>
<td>Packets Out</td>
<td>the number of outgoing packets handled by the protocol through the security</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>previous packets out value.</td>
</tr>
<tr>
<td>Util. (Absolute)</td>
<td>the total number of the utilization of the current security device.</td>
</tr>
<tr>
<td>Util. (Delta)</td>
<td>the total numerical difference between the current utilization value and the</td>
</tr>
<tr>
<td></td>
<td>previous utilization value.</td>
</tr>
<tr>
<td>Zone</td>
<td>the name of the zone associated with the protocol.</td>
</tr>
</tbody>
</table>

**NOTE:** Additional options enable 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 security devices to implement VPNs, you can view how traffic is being distributed across each different VPN tunnel on the security device. A bar graph appears (under the Chart tab) depicting the distribution of data traveling to and from each VPN tunnel. The graph uses a percentage of the absolute number of bytes traveling in to the top 10 VPN tunnels by default.

You can adjust all elements depicted in the graph including the VPN tunnels, data values (absolute or delta), and type of data (bytes in or out, packets in or out, utilization).

**Adjusting VPN Tunnels Depicted Graphically**
1. Right-click the Chart view and select Configure VPNs. A pop-up enabling you to select VPNs appears.
2. Clear the Default checkbox.

3. Click to select the VPN tunnel that you wish to view on the graph from the list of Available VPN tunnels. Click Add to add the VPN tunnel to the list of Selected VPN tunnels.

4. Click to select the VPN tunnel that you no longer wish to view on the graph from the list of Selected VPN tunnels. Click Remove to remove the VPN tunnel from the list of Selected VPN tunnels.

5. Click OK to apply your changes; or click Cancel to cancel your changes.

Adjusting Data Depicted Graphically
1. Right-click the Chart view and select Data, and either Delta or Absolute.

2. Right-click the Chart view and select Data Type, and either Bytes In, Bytes Out, Packets In Packets Out, Utilization, Last Session Duration, Avg Latency, Availability.

3. Click OK to apply your changes; or click Cancel to cancel your changes.

Viewing VPN-specific Information
Click the VPN Monitor Table tab to view specific information about your VPN. From the VPN Monitor Table, you can view the following details about a specific VPN:

- Key details describing the VPN (such as name, Policy ID, group and user associations, VPN type).
- Security Association (SA) information.
- Total number of data over the tunnel (such as bytes in/out, packets in/out, utilization).

The following table describes all of the information that is available from the VPN Monitor Table:

Table 40: VPN Monitor Table

<table>
<thead>
<tr>
<th>Item</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>the name of the VPN.</td>
</tr>
<tr>
<td>VPN Type</td>
<td>Type of tunnel: Site-to-site or dial-up.</td>
</tr>
<tr>
<td>SA Id</td>
<td>the Security Association (SA) identification for the VPN at both ends of the tunnel.</td>
</tr>
<tr>
<td>Policy Id-In/Out</td>
<td>A unique identifier specified when the policy was configured.</td>
</tr>
<tr>
<td>Status</td>
<td>up/down status of the VPN tunnel.</td>
</tr>
<tr>
<td>SA Status</td>
<td>whether or not the current SA has been established.</td>
</tr>
<tr>
<td>Time-SA Status Change</td>
<td>time that the SA status last changed</td>
</tr>
<tr>
<td>Last SA Session Duration</td>
<td>duration of last SA session</td>
</tr>
<tr>
<td>Group</td>
<td>Group associated with the VPN.</td>
</tr>
<tr>
<td>User</td>
<td>User associated with the VPN.</td>
</tr>
</tbody>
</table>
Viewing Active VPN Information

Click the Active VPN tab to view specific information about active VPNs. From the Active VPN, you can view the following details:

- Key details describing the VPN (such as name, Policy IP, local and peer gateway IDs and IP addresses).
- Security established on the active VPN.
- Time-related statistics (such as lifetime, latency).

Table 41 lists the information that is available from the active VPN.

**Table 41: Active VPN Table**

<table>
<thead>
<tr>
<th>Item</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>DN Name</td>
<td>Distinguished Name (DN) of the VPN.</td>
</tr>
<tr>
<td>Avg. Latency</td>
<td>A rolling average of latency, presented in milliseconds.</td>
</tr>
<tr>
<td>Availability</td>
<td>Percentage of the time a tunnel is up over the last thirty samples.</td>
</tr>
<tr>
<td>Bytes In</td>
<td>the number of incoming bytes handled by the protocol through the security device.</td>
</tr>
<tr>
<td>Delta Bytes In</td>
<td>Total numerical difference between the current bytes in value and the previous bytes in value.</td>
</tr>
<tr>
<td>Bytes Out</td>
<td>the number of outgoing bytes handled by the protocol through the security device.</td>
</tr>
<tr>
<td>Delta Bytes Out</td>
<td>Total numerical difference between the current bytes out value and the previous bytes out value.</td>
</tr>
<tr>
<td>Packets In</td>
<td>the number of incoming packets handled by the protocol through the security device.</td>
</tr>
<tr>
<td>Delta Packets In</td>
<td>Total numerical difference between the current packets in value and the previous packets in value.</td>
</tr>
<tr>
<td>Packets Out</td>
<td>the number of outgoing packets handled by the protocol through the security device.</td>
</tr>
<tr>
<td>Delta Packets Out</td>
<td>Total numerical difference between the current packets out value and the previous packets out value.</td>
</tr>
<tr>
<td>Util. (Absolute)</td>
<td>Total number of the utilization of the current security device.</td>
</tr>
<tr>
<td>Util. (Delta)</td>
<td>Total numerical difference between the current utilization value and the previous utilization value.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Item</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>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>Tunnel status for the active VPN is UP or Down.</td>
</tr>
<tr>
<td>Ave Latency</td>
<td>Rolling average latency (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 time a tunnel is available over the last 30 samples.</td>
</tr>
</tbody>
</table>
Viewing Interface Statistics
You can also view traffic information as it is processed by a device on a specific interface:

- Viewing Ethernet Statistics
- Viewing Flow Statistics
- Viewing Attack Statistics

Viewing Ethernet Statistics
Click the Ethernet Statistics node to view traffic information as it is processed by a specific physical interface on a security device. Depending upon the specific security device, the following interfaces apply:

- Trust and Untrust interfaces available on all security devices.

<table>
<thead>
<tr>
<th>Item</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local GW Id</td>
<td>Local gateway ID for the active VPN.</td>
</tr>
<tr>
<td>Peer GW Id</td>
<td>Peer gateway ID for the active VPN.</td>
</tr>
<tr>
<td>Local GW IP</td>
<td>Local gateway IP address for the active VPN.</td>
</tr>
<tr>
<td>Peer GW IP</td>
<td>Peer gateway IP address for the active VPN.</td>
</tr>
<tr>
<td>Local Address</td>
<td>Local IP address for the security device associated to the active VPN.</td>
</tr>
<tr>
<td>Peer Address</td>
<td>Peer IP address for the security device connected to the active VPN.</td>
</tr>
<tr>
<td>Monitor</td>
<td>Monitoring capability status for the VPN: ON or OFF.</td>
</tr>
<tr>
<td>IPSec</td>
<td>IPSec (IP security) protocol for the active VPN; AH (Authentication Header) or ESP (Encapsulating Security Payload).</td>
</tr>
<tr>
<td>SPI In</td>
<td>SPI (Security Parameter Index) key into the active VPN. A value that identifies a security association (SA).</td>
</tr>
<tr>
<td>SPI Out</td>
<td>SPI (Security Parameter Index) key out of the active VPN. A value that identifies an SA.</td>
</tr>
<tr>
<td>Encryption</td>
<td>Algorithm used when a user encrypts communication between the security device and the server. Listed as either SDI or DES.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Second algorithm used for user encrypted communication between the security device and server.</td>
</tr>
<tr>
<td>Key</td>
<td>Type of key associated with the VPN: Auto IKE (Internet Key Exchange) or manual key.</td>
</tr>
<tr>
<td>Lifetime P1</td>
<td>Time listed in seconds before re-keying.</td>
</tr>
<tr>
<td>Lifetime P2</td>
<td>Time reported in remaining bytes before re-keying. Independent from Lifetime P1.</td>
</tr>
<tr>
<td>Life Size</td>
<td>Predefined duration of the tunnel (in bytes).</td>
</tr>
<tr>
<td>P1 Status</td>
<td>P1 (phase 1) status for tunnel negotiation: enabled or disabled.</td>
</tr>
<tr>
<td>P2 Status</td>
<td>P2 (phase 2) status for tunnel negotiation: enabled or disabled.</td>
</tr>
<tr>
<td>P1 Auth</td>
<td>Associated with Auto IKE. This column displays the P1 (phase 1) authentication for the active VPN.</td>
</tr>
</tbody>
</table>
- DMZ interface available on NetScreen-25, NetScreen-50, NetScreen-100 and NetScreen-500 devices; the NetScreen-5XP device has no DMZ interface.

- HA interface and management interface available on NetScreen-100 and NetScreen-500 devices.

Ethernet Statistics apply only to security devices, and not to virtual systems.

A graph appears displaying security device % utilization traffic on the interface. Right-click within the chart to select a desired Interface (such as Ethernet or HA). The active interface is listed below the graph. The graph will also provide the total errors in a graphical form. You can view up to 12 samples in the chart. The following table describes the information available from the Ethernet Statistics view:

Table 42: Ethernet Statistics View Data

<table>
<thead>
<tr>
<th>Item</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>the data for each interface.</td>
</tr>
<tr>
<td>Bytes In</td>
<td>the number of bytes of incoming traffic processed through the security device over the selected interface.</td>
</tr>
<tr>
<td>Delta Bytes In</td>
<td>the total numerical difference between the current bytes in value and the previous bytes in value.</td>
</tr>
<tr>
<td>Bytes Out</td>
<td>the number of outgoing bytes handled by the interface through the security device.</td>
</tr>
<tr>
<td>Delta Bytes Out</td>
<td>the total numerical difference between the current bytes out value and the previous bytes out value.</td>
</tr>
<tr>
<td>Packets In</td>
<td>the number of incoming packets handled by the interface through the security device.</td>
</tr>
<tr>
<td>Delta Packets In</td>
<td>the total numerical difference between the current packets in value and the previous packets in value.</td>
</tr>
<tr>
<td>Packets Out</td>
<td>the number of outgoing packets handled by the interface through the security device.</td>
</tr>
<tr>
<td>Delta Packets Out</td>
<td>the total numerical difference between the current packets out value and the previous packets out value.</td>
</tr>
<tr>
<td>Broadcast</td>
<td>the number of broadcast-type packets processed through the security device over the selected interface.</td>
</tr>
<tr>
<td>CRC Errors</td>
<td>the number of packets generating a cyclic redundancy code error processed through the security device over the selected interface.</td>
</tr>
<tr>
<td>Alignment Errors</td>
<td>the number of Frame Checksum (FCS) errors.</td>
</tr>
<tr>
<td>ShortFrame</td>
<td>the number of frames that are not of the correct length.</td>
</tr>
<tr>
<td>RXCollision</td>
<td>the number of times that two packets collide, resulting in damage to both. This indicates that the network is overloaded.</td>
</tr>
<tr>
<td>Speed (Mbps)</td>
<td>This is useful in calculating the speed of the interface.</td>
</tr>
<tr>
<td>Status</td>
<td>whether the security device is currently Up or Down.</td>
</tr>
<tr>
<td>Direction</td>
<td>whether the security device is in half or full duplex mode.</td>
</tr>
<tr>
<td>Zone</td>
<td>the name of the zone associated with the interface.</td>
</tr>
</tbody>
</table>
**Viewing Flow Statistics**

Click the Flow Statistics node to view data for various flow counters on a specific security device or virtual interface. For each security device, the data and statistics are separated by all available interfaces.

You can change the interface setting by right-clicking in the chart and selecting the interface that you want. The following table describes all of the information that is available from the Flow Statistics view:

Table 43: Flow Statistics View Data

<table>
<thead>
<tr>
<th>Item</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>the name of the virtual interface</td>
</tr>
<tr>
<td>Bytes In</td>
<td>the number of bytes of incoming traffic processed through the security device over the selected interface.</td>
</tr>
<tr>
<td>Bytes Out</td>
<td>the number of bytes of outgoing traffic processed through the security device over the selected interface.</td>
</tr>
<tr>
<td>Packets In</td>
<td>the number of incoming packets processed through the security device over the selected interface.</td>
</tr>
<tr>
<td>Packets Out</td>
<td>the number of outgoing packets processed through the security device over the selected interface.</td>
</tr>
<tr>
<td>VLAN In</td>
<td>the number of VLAN packets received through the security device; applies to virtual systems.</td>
</tr>
<tr>
<td>VLAN Out</td>
<td>the number of VLAN packets sent through the security device; applies to virtual systems.</td>
</tr>
<tr>
<td>Connections</td>
<td>the number of connections that occurred for a given interface.</td>
</tr>
<tr>
<td>Packets Dropped</td>
<td>the number of incoming packets dropped by a given interface.</td>
</tr>
<tr>
<td>Packets Denied</td>
<td>the number of incoming packets denied on the virtual interface by the policy.</td>
</tr>
<tr>
<td>Authentication Failed</td>
<td>the number of packets dropped because of an authentication failure.</td>
</tr>
<tr>
<td>URL Blocking Dropped</td>
<td>the number of packets dropped because of URL blocking.</td>
</tr>
<tr>
<td>IPSec Dropped</td>
<td>the number of IPSec packets dropped.</td>
</tr>
<tr>
<td>Zone</td>
<td>the name of the zone associated with the interface.</td>
</tr>
</tbody>
</table>

**Viewing Attack Statistics**

Click the Attack Statistics node to view distribution of the attacks that have occurred on a specific security device. The report separates the data and statistics for all available interfaces. The following table describes each of the attack counters available from the Attack Statistics view:

Table 44: Attack Counters

<table>
<thead>
<tr>
<th>Item</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Name of the interface.</td>
</tr>
<tr>
<td>SYN Attack</td>
<td>SYN packets overwhelm a network by initiating so many connection attempts or information requests that the network can no longer process legitimate connection requests, resulting in a Denial of Service.</td>
</tr>
<tr>
<td>Item</td>
<td>Displays...</td>
</tr>
<tr>
<td>--------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Tear Drop</td>
<td>When the first and second parts of a fragmented packet overlap, the server attempting to reassemble the packet can crash. If the security device sees this discrepancy in a fragmented packet, it drops the packet.</td>
</tr>
<tr>
<td>Source Route</td>
<td>This option applies in an IP header and allows an attacker to enter a network with a false IP address and have data sent back to the attacker's real address.</td>
</tr>
<tr>
<td>Ping of Death</td>
<td>Intentionally oversized or irregular ICMP packets can trigger a Denial of Service condition, freezing, or other adverse system reactions. You can configure a security device to detect and reject oversized or irregular packet sizes.</td>
</tr>
<tr>
<td>Address Spoofing</td>
<td>You can enable a security device to guard against spoofing attacks by checking its own route table. If the IP address is not in the route table, traffic through the security device is not allowed.</td>
</tr>
<tr>
<td>Land Attack</td>
<td>Combining a SYN attack with IP spoofing, a Land attack occurs when an attacker sends spoofed SYN packets containing the IP address of the victim as both the destination and source IP address. This creates an empty connection. Flooding a system with such empty connections can overwhelm the system, causing a Denial of Service. Security devices automatically block any attempt of this nature and records such attempts as a Land attack.</td>
</tr>
<tr>
<td>ICMP Flood</td>
<td>ICMP pings can be so numerous that they overload a system with so many echo requests that the system expends all its resources responding until it can no longer process valid network traffic. If you set a threshold to invoke ICMP flood attack protection when exceeded, ICMP flood attacks are recorded as statistics.</td>
</tr>
<tr>
<td>UDP Flood</td>
<td>Similar to the ICMP flood, UDP flooding occurs when UDP packets are sent with the purpose of slowing down the system to the point that it can no longer handle valid connections. After enabling the UDP flood protection feature, you can set a threshold that once exceeded invokes the UDP flood attack protection feature. (The default threshold value is 1000 packets per second.) If the threshold is exceeded, the security device ignores further UDP packets for the remainder of that second.</td>
</tr>
<tr>
<td>Port Scan</td>
<td>Port scan attacks occur when packets are sent with different port numbers with the purpose of scanning the available services in hopes that one port will respond. The security device internally logs the number of different ports scanned from one remote source. If a remote host scans 10 ports in 0.3 seconds, Juniper Networks flags this as a port scan attack, and rejects further packets from the remote source.</td>
</tr>
<tr>
<td>IP Sweep</td>
<td>This is the same as an address sweep attack, and similar to a port scan attack. It occurs when an attacker sends ICMP echo requests (pings) to different destination addresses hoping that one will reply, thus uncovering an address to a target. If a remote host pings 10 addresses in 0.3 seconds, the security device flags this as an address sweep attack and drops the connection.</td>
</tr>
<tr>
<td>Block Java/ActX</td>
<td>Malicious Java or ActiveX components can be hidden in Web pages. When downloaded, these applets install a Trojan horse on your computer. Similarly, Trojan horses can be hidden in compressed files such as .zip, .gzip, and .tar, and executable (.exe) files.</td>
</tr>
</tbody>
</table>
### Item | Displays...
--- | ---
SYN Frag | A SYN fragment attack floods the target host with SYN packet fragments. The host catches the fragments, waiting for the remaining packets to arrive so it can reassemble them. By flooding a server or host with connections that cannot be completed, the host's memory buffer eventually fills. No further connections are possible, and damage to the host’s operating system can occur. The security device drops ICMP packets when the protocol field indicates ICMP packets, and the fragment flag is set to 1 or an offset is indicated.
TCP no Flag | TCP packet that does not have any bits set in the flags.
Unknown Prot | The security device drops packets where the protocol field is set to 101 or greater. These protocol types are reserved and undefined at this time.
Bad IP Opt | Triggered when the list of IP options in the IP datagram header is incomplete or malformed.
IP Rec Route | The security device blocks packets where the IP option is 7 (Record Route). This option is used to record the route of a packet. A recorded route is composed of a series of internet addresses, which an outsider can analyze to learn details about your network’s addressing scheme and topology.
IP Timestamp | The security device blocks packets where the IP option list includes option 4 (Internet Timestamp).
IP Security | This option provides a way for hosts to send security, compartmentation, TCC (closed user group) parameters, and Handling Restriction Codes compatible with DOD requirements.
IP Loose Src | The security device blocks packets where the IP option is 3 (Loose Source Routing). This option provides a means for the source of a packet to supply routing information to be used by the gateways in forwarding the packet to the destination. This option is a loose source route because the gateway or host IP is allowed to use any route of any number of other intermediate gateways to reach the next address in the route.
IP Strict Src | The security device blocks packets where the IP option is 9 (Strict Source Routing). This option provides a means for the source of a packet to supply routing information to be used by the gateways in forwarding the packet to the destination. This option is a strict source route because the gateway or host IP must send the datagram directly to the next address in the source route, and only through the directly connected network indicated in the next address to reach the next gateway or host specified in the route.
IP Stream | The security device blocks packets where the IP option is 8 (Stream ID). This option provides a way for the 16-bit SATNET stream identifier to be carried through networks that do not support the stream concept.
ICMP Frag | When the protocol field indicates ICMP packets, and the fragment flag is set to 1 or an offset is indicated.
Large ICMP | An ICMP packet with a length greater than 1024.
SYN n FIN | Both the SYN and FIN flags are not normally set in the same packet. However, an attacker can send a packet with both flags set to see what kind of system reply is returned and thereby determine what kind of system is on the receiving end. The attacker can then use any known system vulnerabilities for further attacks. Enable this option to have the security device drop packets that have both the SYN and FIN bits set in the flags field.
FIN no ACK | TCP packet with a FIN set but no ACK set in the flags field.
Mal URL | When you enable Malicious URL Detection, the security device monitors each HTTP packet and detects any URL that matches any of several user-defined patterns. The security device automatically drops any such packet.
Monitoring Security Devices

Viewing Zone Statistics
You can also view traffic information as it is processed by a security device over specific zones. You can view ethernet statistics, flow statistics and attack statistics in the same manner that you viewed them in the Interface reports according to zone.

Viewing System Statistics
You can also view system-related information for a security device.

Viewing Resource Statistics
Click the Resource Statistics node to view the resources for a security device. The following table describes all of the information that is available from the Resource Statistics view:

Table 45: Resource Statistics Items

<table>
<thead>
<tr>
<th>Item</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avg. CPU Utilization</td>
<td>the average CPU usage of the security device.</td>
</tr>
<tr>
<td>Memory Allocated</td>
<td>the current memory allocation to security device.</td>
</tr>
<tr>
<td>Memory Left</td>
<td>the remaining usable memory.</td>
</tr>
<tr>
<td>No. of Fragment Blocks</td>
<td>a percentage of blocks that are fragmented.</td>
</tr>
<tr>
<td>Active Sessions</td>
<td>the number of currently active sessions.</td>
</tr>
<tr>
<td>Allocated Sessions</td>
<td>the number of allocated sessions.</td>
</tr>
<tr>
<td>Max. Sessions Allowed</td>
<td>the maximum sessions allowed.</td>
</tr>
<tr>
<td>Failed Sessions</td>
<td>the number of sessions that failed to allocate (after maximum reached).</td>
</tr>
</tbody>
</table>

Limit Session
Security 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 security device can establish per second for a single IP address. (The default threshold is 128 sessions per second per IP address.)

Block Frag
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 security device to deny IP fragments on a security zone, the security device blocks all IP packet fragments that it receives at interfaces bound to that zone.

Zone
the name of the zone associated with the attack.
Viewing Active Statistics

Click the Active Statistics node to view administrator and user activities for a security device. The Administrators tab displays information about the administrators, including when, where, and how they logged in to the system. The following table describes all of the information that is available from the Administrators view:

Table 46: Administrators View

<table>
<thead>
<tr>
<th>Item</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator ID</td>
<td>the administrator’s logon ID.</td>
</tr>
<tr>
<td>IP Address</td>
<td>the administrator’s IP address.</td>
</tr>
<tr>
<td>Service Used</td>
<td>the type of service, for example, Console, Web, or Telnet to login.</td>
</tr>
<tr>
<td>Time</td>
<td>the time that the administrator logged on.</td>
</tr>
</tbody>
</table>

The following table describes all of the information that is available from the Authenticated Users view:

Table 47: Authenticated Users View

<table>
<thead>
<tr>
<th>Item</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID</td>
<td>User log in ID.</td>
</tr>
<tr>
<td>Source IP Address</td>
<td>Source IP address.</td>
</tr>
<tr>
<td>Time</td>
<td>Time that the user logged on.</td>
</tr>
</tbody>
</table>

You can also access VPN information from the Active VPN view, and Active Session information from the Active Sessions view.

Viewing Active Sessions

You can view a snapshot of ongoing active sessions on the security device. You can view active sessions from the Active Statistics view.

When you click the Active Sessions tab, a short form view of the active sessions appears, enabling you to monitor basic information (such as source IP, destination IP, translated IP (if applicable), source port, destination port, translated port (if applicable), policy ID, time the session starts, and protocol type) about the active sessions on the security device by default. You can also view extended information about the session, such as session ID, ICMP type (if applicable), total incoming bytes, total outgoing bytes, total packets count, how long the session has been active.

The following table describes all of the information that is available from the Active Sessions view:

Table 48: Active Sessions Items

<table>
<thead>
<tr>
<th>Item</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session ID</td>
<td>A unique identifier specified with the active session.</td>
</tr>
<tr>
<td>Source IP</td>
<td>IP address of the sending node of the connection.</td>
</tr>
</tbody>
</table>
Using the Session Filter

You can control the information that is provided in the Active Sessions view by configuring a session filter. Using the Session Filter, you can fetch specific sessions on a security device that match specific criteria that you set. Like the Monitor Filter for the Event Summary View, there is only one Session Filter and it defines the overall data set that you can view from the Active Sessions view. After you have configured and applied the Session Filter, you can then configure additional session display filters to view more specific session information.

Configuring the Session Filter

To configure the session filter:

1. Use the Options menu, and select Session Filter. The Session Filter Dialog will appear.

2. Click in the Long Form checkbox to display additional information about the Active Session.

3. Click in the Maximum number of sessions to retrieve checkbox and enter the total number of sessions you want the Session Filter to retrieve.

4. Specify criteria for the sessions that you would like to view. You can specify an active session according to the following:

   - Source, Destination, and Translated IP (IP Address, Net Mask, and Port Range)
   - Session Duration
   - Session Start Date and Time

<table>
<thead>
<tr>
<th>Item</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<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>
- Policy ID
- Session Type
- Protocol ID
- Policy with Logging

5. Click More to view additional criteria.

6. Click Reset to Default to reset all criteria back to their default settings.

7. Click OK when you are done.

8. Click Refresh to apply the criteria to the active session table view.

**Configuring a Session Display Filter**
You can apply a session display filter to view only specific active sessions.

1. Use the Options menu, and select Session Display Filter. The Session Filter Dialog will appear.

2. From the Source tab, you can specify the sessions that you want to view according to the Source IP Address and Port number, or Port Range.

3. Click in the Destination tab to specify the sessions that you want to view according to Destination IP Address and Port number, or Port Range.

4. Click in the Translated tab to specify the sessions that you want to view according to Translated IP Address and Port number, or Port Range.

5. Click in the Protocol tab specify the sessions that you want to view according to protocol.

6. Click in the Other tab specify the sessions that you want to view according to Session Duration, Session Start Time or Policy ID.

7. Click OK when you are done.

8. Click Refresh to apply the Session Display criteria to the active session table view.

**Troubleshooting**
From the Device Monitor, you can right-click on any security device and select the Troubleshoot option to issue common CLI commands (i.e., get, exec, debug) to a security device using Telnet or a Secure Command Shell to troubleshoot problems. You can also add and delete CLI commands to the list of commands available by using the **Add/Delete Custom Troubleshoot Commands** option under the **Tools** menu in the UI.

To troubleshoot a device:
1. From the Device Monitor, right-click on any device and select Troubleshoot. The Troubleshoot Device window appears.

2. Select the appropriate command from the list of Predefined Commands in the Shortcuts window. The command(s) appear in the Command field.

3. Click on the Execute Command button. The status of the command appears in the field below. Note all commands that you execute appear in the History window.

For your convenience, you can add or remove specific commands as a Shortcut in the Shortcuts window.

NOTE: Commands from NetScreen-Security Manager originate from the UI client to the security device. If you intend to issue get commands from NetScreen-Security Manager, you must plan and implement Security Policy rules in your network accordingly.

Viewing High Availability (HA) Statistics (if applicable)

If you have configured security devices to be highly available, you can view NSRP-related statistics on the device by accessing the HA Statistics view. The following table describes all of the information that is available from the HA Statistics view:

Table 49: HA Statistics View

<table>
<thead>
<tr>
<th>Item</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>VSD Group ID</td>
<td>the group ID that is associated with the VSD (or RTO).</td>
</tr>
<tr>
<td>Number of Units</td>
<td>the number of units associated with the VSD (or RTO).</td>
</tr>
<tr>
<td>State Change Counter</td>
<td>the number of times a security device changes operational states.</td>
</tr>
<tr>
<td>Init Counter</td>
<td>the transient state of a VSD (or RTO) group member while it was in the process of joining the VSD (or RTO) group.</td>
</tr>
<tr>
<td>Master</td>
<td>the number of Master security devices.</td>
</tr>
<tr>
<td>Primary BackUp</td>
<td>the number of primary backup security devices.</td>
</tr>
<tr>
<td>BackUp</td>
<td>the total number of backup security devices.</td>
</tr>
<tr>
<td>Ineligible</td>
<td>Notes that an administrator purposefully assigned a security device so that it cannot participate in the selecting a new master security device.</td>
</tr>
<tr>
<td>InOperable</td>
<td>Notes that a VSD (or RTO) group security device has an internal problem.</td>
</tr>
<tr>
<td>Master Conflict</td>
<td>the number of conflicts that occurred on the master security device.</td>
</tr>
<tr>
<td>Primary Backup Conflict</td>
<td>the number of conflicts that occurred on the primary backups security device.</td>
</tr>
<tr>
<td>Tx Heartbeat</td>
<td>the number of transmitted heartbeats on the security devices.</td>
</tr>
<tr>
<td>Rx Heartbeat</td>
<td>the number of received heartbeats on the security devices.</td>
</tr>
</tbody>
</table>
Monitoring IDP Sensors

Use the Device Monitor to get an at-a-glance view of the current status of all the IDP sensors in your network.

If you have configured multiple sub-domains, you can view all your managed devices from the global domain.

Viewing IDP Device Status

The following table lists and describes information about IDP sensors that you can view through the Device Monitor:

Table 50: Device Status Information

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name assigned to the sensor in NetScreen-Security Manager</td>
</tr>
<tr>
<td>Domain</td>
<td>Domain in NetScreen-Security Manager in which the sensor is managed. <strong>Note:</strong> If you have configured multiple sub-domains, you can view all your managed devices from the global domain.</td>
</tr>
<tr>
<td>Device Type</td>
<td>Model number of the sensor.</td>
</tr>
<tr>
<td>Managed OS Version</td>
<td>IDP firmware version running on the sensor.</td>
</tr>
<tr>
<td>Config Status</td>
<td>Displays the current configuration status of the sensor in NetScreen-Security Manager:</td>
</tr>
<tr>
<td></td>
<td>- None. No state has been set (does not show in Device Monitor).</td>
</tr>
<tr>
<td></td>
<td>- Modeled. The sensor exists in NetScreen-Security Manager, but a connection to the sensor has not yet been established.</td>
</tr>
<tr>
<td></td>
<td>- RMA. Equivalent to bringing the sensor into the Modeled state. RMA results from an admin selection in the User Interface when a sensor goes down.</td>
</tr>
<tr>
<td></td>
<td>- Waiting for 1st connect. NetScreen-Security Manager is waiting for the sensor to connect. You must enter a command on the sensor to make it connect to NetScreen-Security Manager.</td>
</tr>
<tr>
<td></td>
<td>- Import Needed. You must import the configuration of the sensor into NetScreen-Security Manager. When you add a sensor for the first time, verify that your status indicates “Import Needed” before you attempt to import the sensor. During migration, this state indicates that import of the sensor configuration is still required.</td>
</tr>
<tr>
<td></td>
<td>- Await Migration. After you have migrated your data in IDP Manager, the Config Status on each sensor displays that it is awaiting migration. It remains in this state until you have migrated the sensor.</td>
</tr>
<tr>
<td></td>
<td>- Update Needed. An update to this sensor is required.</td>
</tr>
<tr>
<td></td>
<td>- Managed. The sensor is currently being managed by NetScreen-Security Manager.</td>
</tr>
</tbody>
</table>
Viewing IDP Device Detail and Statistics

If a sensor is up and running, you can also access additional information on the
device. To view additional status, you can view Device Details. For traffic-related
statistics and other information, you can View Statistics.

NOTE: If a sensor is never connected, the Device Detail Status and Statistics views for the
sensor are not available.

Viewing IDP Device Details

Double-click on any IDP sensor to view additional details on the sensor related to
resource usage. You can also right-click on the sensor and select View Details.

NOTE: The information in the Details window appears slightly different for firewall/VPN
devices and IDP sensors. Details for IDP sensors also include an additional tab
enabling you to view process status.

The following table lists and describes the information that you can view for an IDP
sensor 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 IDP firmware version running on the sensor.</td>
</tr>
<tr>
<td>Mode</td>
<td>Current operation mode of the device.</td>
</tr>
</tbody>
</table>
Chapter 12: Realtime Monitoring

Viewing IDP Process Status

For IDP sensors, use the Process Status tab to view information on various processes running on the sensor.

Figure 173: Process Status for IDP Sensor

The following table lists and describes the information that you can view for an IDP sensor through the Process Status:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU Idle</td>
<td>Percentage of the time the CPU was idle.</td>
</tr>
<tr>
<td>CPU User</td>
<td>Percentage of CPU utilization that occurred while executing at the user level.</td>
</tr>
<tr>
<td>CPU Kernel</td>
<td>Percentage of CPU utilization that occurred while executing at the system level.</td>
</tr>
<tr>
<td>CPU Usage</td>
<td>Percentage of CPU utilization.</td>
</tr>
<tr>
<td>1 Min. Load</td>
<td>One minute load average.</td>
</tr>
<tr>
<td>5 Min. Load</td>
<td>Five minute load average.</td>
</tr>
<tr>
<td>15 Min. Load</td>
<td>Fifteen minute load average.</td>
</tr>
<tr>
<td>Total Mem</td>
<td>Total amount (in megabytes) of memory.</td>
</tr>
<tr>
<td>Used Mem</td>
<td>Amount (in megabytes) of used memory.</td>
</tr>
<tr>
<td>Mem Usage</td>
<td>Percentage of used memory.</td>
</tr>
<tr>
<td>Total Swap</td>
<td>Total amount (in megabytes) of swap space.</td>
</tr>
<tr>
<td>Used Swap</td>
<td>Amount (in megabytes) of used swap space.</td>
</tr>
<tr>
<td>Swap Usage</td>
<td>Percentage of used swap space.</td>
</tr>
</tbody>
</table>
Table 52: IDP Sensor Process Status Items

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process Name</td>
<td>Name of the process running on the sensor.</td>
</tr>
<tr>
<td>Total Mem Usage</td>
<td>Amount (in megabytes) of memory used.</td>
</tr>
<tr>
<td>Phys Mem Usage</td>
<td>Amount of memory (in kilobytes) a process currently has in physical memory (not in swap).</td>
</tr>
<tr>
<td>CPU Usage</td>
<td>Percentage of CPU used.</td>
</tr>
</tbody>
</table>

Viewing IDP Device Statistics

If a sensor is up and running, you can also access the Statistics view to access traffic and other system-related information on the device. To view statistics on a particular sensor, right-click the sensor in either the Device Monitor or the Device Manager and select View Statistics. The Device Statistics Summary appears in a new window.

Figure 174: Device Statistics Summary for IDP Sensor

NOTE: The information in the Device Statistics window appears slightly different for firewall/VPN devices and IDP sensors.

IDP Device Statistics Summary

The Device Statistics Summary displays the following details:

- Details describing the sensor, for example, firmware version and mode.
- Packet and Flow information

The following table details additional information you can view from the Device Statistics Summary for IDP sensors.
Monitoring VPNs

Use VPN Monitor to get an at-a-glance status of the up/down status of VPN tunnels as well as other statistics relevant to your VPN.

**Figure 175: Monitoring VPNs**

<table>
<thead>
<tr>
<th>Item</th>
<th>Displays</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS Version</td>
<td>Indicates the IDP firmware version running on the sensor.</td>
</tr>
<tr>
<td>Mode</td>
<td>Current operation mode of the device.</td>
</tr>
<tr>
<td>ICMP Packets</td>
<td>Total number of ICMP packets.</td>
</tr>
<tr>
<td>TCP Packets</td>
<td>Total number of TCP packets.</td>
</tr>
<tr>
<td>UDP Packets</td>
<td>Total number of UDP packets.</td>
</tr>
<tr>
<td>Other Packets</td>
<td>Total number of other packets.</td>
</tr>
<tr>
<td>ICMP Flows</td>
<td>Total number of ICMP flows.</td>
</tr>
<tr>
<td>TCP Flows</td>
<td>Total number of TCP flows.</td>
</tr>
<tr>
<td>UDP Flows</td>
<td>Total number of UDP flows.</td>
</tr>
<tr>
<td>Other Flows</td>
<td>Total number of other flows.</td>
</tr>
</tbody>
</table>

**NOTE:** You must enable the “VPN Monitor” option on the tunnel when configuring the tunnel for the device.

Viewing the VPN Status Summary

The VPN Monitor lists a summary of all the VPN tunnels that have been implemented in your system. It includes visual indicators that depict whether an existing VPN tunnel is either Up, Down, or Not Monitored. The Summary also includes information describing the VPN name, VPN type, Source, Destination, Security Parameter Index., IP Address, and Protocol.
Table 54: VPN Tunnel Summary

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN</td>
<td>Name of the active VPN.</td>
</tr>
<tr>
<td>VPN Type</td>
<td>Type of tunnel: Dialup or Site to Site.</td>
</tr>
<tr>
<td>From Hostname(IP(Vsys)</td>
<td>Source security devices used in the VPN. For example, a root security device named NS5000 with an IP address of 1.1.1.1 appears as NS5000(1.1.1.1). For a Vsys 1, “NS5000(1.1.1.1)(1)” appears.</td>
</tr>
<tr>
<td>From Domain</td>
<td>Domain in NetScreen-Security Manager in which the source security device used in the VPN is managed.</td>
</tr>
<tr>
<td>To Hostname(IP(Vsys))</td>
<td>Destination security devices used in the VPN. For example, a root security device named NS5000 with an IP address of 1.1.1.1 appears as NS5000(1.1.1.1). For a Vsys 1, “NS5000(1.1.1.1)(1)” appears.</td>
</tr>
<tr>
<td>To Domain</td>
<td>Domain in NetScreen-Security Manager in which the destination security device used in the VPN is managed.</td>
</tr>
<tr>
<td>Status</td>
<td>VPN Status: Up or Down</td>
</tr>
<tr>
<td>SPI (in/out)</td>
<td>Security Parameter Index (SPI) key into and out of the active VPN. This is the encryption method.</td>
</tr>
<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>

Configuring a VPN Display Filter

You can control the information that is provided in the VPN Monitor by configuring a VPN display filter. Use the Options menu and select Display Filter to configure a VPN display filter. The VPN Display filter provides several options enabling you to view VPN information related to the type, status, or the specific security device or virtual system associated with the VPN tunnel that you want to view. Click the Refresh button to apply the Session Display criteria to the active session table view.

Viewing Active VPN Details

To view the details on the active VPN, click to select the VPN, use the View menu and select Active VPN Details (alternatively, you can also right-click the VPN tunnel and select Active VPN Details).

Refer to “Viewing Active VPN Information” on page 530 for more information on the Active VPN Details table.

Viewing Device-Specific VPN Information

Right-click the VPN tunnel and select Monitor Data, and then the security device to view security device-specific information about your VPN. A Monitor info window appears where you can access the VPN Monitor table, Active VPN table, and a chart enabling you to view the distribution of VPN tunnels on the security device.
Monitoring NSRP Statistics

If you have implemented NetScreen Redundancy Protocol (NSRP) for the purpose of deploying clusters for redundancy, you can use the NSRP Monitor to get an at-a-glance status of your Juniper Networks systems that are in “clusters.” These systems include both the NetScreen-500 and the NetScreen-1000. To launch the NSRP Monitor, click NSRP Monitor.

Viewing NSRP Summary Information

Double-click an NSRP device to view a summary of the top-level information on the selected cluster. From the NSRP Summary, you can view the following details about a specific cluster:

- Key details describing the cluster (such as name, # of VSDs, # of RTOs)
- Security details
- The total number and type of events

The following table describes all of the information that is available from the NSRP summary:

Table 55: NSRP Device Summary

<table>
<thead>
<tr>
<th>Item</th>
<th>Displays…</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster</td>
<td>name of this cluster.</td>
</tr>
<tr>
<td>Domain</td>
<td>Domain in NetScreen-Security Manager in which the NSRP device is managed.</td>
</tr>
<tr>
<td>No of VSD’s</td>
<td>the total number of Virtual security devices (VSD) that are attached to this cluster.</td>
</tr>
<tr>
<td>No of RTO’s</td>
<td>the total number of Run Time Objects (RTO) that are attached to this cluster.</td>
</tr>
<tr>
<td>Encryption</td>
<td>whether or not encryption has been enabled/disabled.</td>
</tr>
<tr>
<td>Authentication</td>
<td>whether or not authentication has been enabled/disabled.</td>
</tr>
<tr>
<td>No. of Gratuitous arps</td>
<td>the number of gratuitous arps.</td>
</tr>
<tr>
<td>Critical Events</td>
<td>the total number of Critical events that occurred.</td>
</tr>
<tr>
<td>Major Events</td>
<td>the total number of Major events that occurred.</td>
</tr>
<tr>
<td>Minor Events</td>
<td>the total number of Minor events that occurred.</td>
</tr>
<tr>
<td>Warning Events</td>
<td>the total number of Warning events that occurred.</td>
</tr>
<tr>
<td>Intermediate Events</td>
<td>the total number of Intermediate events that occurred.</td>
</tr>
<tr>
<td>Clear Events</td>
<td>the total number of Clear events that occurred.</td>
</tr>
</tbody>
</table>

Viewing VSD/RTO Information

Double-click the cluster security device icon or click the + icon that corresponds to the cluster security device icon to view the virtual security devices (VSD) and run-time objects (RTO) that have been attached to this cluster.
Click the VSD or RTO icon and summary information describing the object appears. The following table describes the information available from the VSD/RTO summary:

Table 56: VSD/ RTO Summary

<table>
<thead>
<tr>
<th>Item</th>
<th>Displays</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster</td>
<td>the name of the cluster associated with this VSD.</td>
</tr>
<tr>
<td>VSD(RTO)</td>
<td>the name of this VSD (or RTO).</td>
</tr>
<tr>
<td>No of Devices</td>
<td>the total number of security devices that are associated with this VSD.</td>
</tr>
<tr>
<td>Init Hold Time</td>
<td>the initial hold time state (in seconds) of the VSD.</td>
</tr>
<tr>
<td>Heartbeat Interval</td>
<td>the time interval (in milliseconds) between each heartbeat.</td>
</tr>
<tr>
<td>Heartbeat Lost Threshold</td>
<td>threshold level required to change over to the backup security device.</td>
</tr>
<tr>
<td>Master</td>
<td>the Master System.</td>
</tr>
<tr>
<td>Primary Backup</td>
<td>the Primary System.</td>
</tr>
</tbody>
</table>

Viewing VSD Counter Details

Click the Counters tab to view specific information about your VSD counters. The following table describes the information that is available from the VSD counters view:

Table 57: VSD Counter Details

<table>
<thead>
<tr>
<th>Item</th>
<th>Displays</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>the device(s) that are associated with the VSD (or RTO).</td>
</tr>
<tr>
<td>Number of Units</td>
<td>the number of units associated with the VSD (or RTO).</td>
</tr>
<tr>
<td>State Change Counter</td>
<td>the number of times a device changes operational states.</td>
</tr>
<tr>
<td>Init Counter</td>
<td>the transient state of a VSD (or RTO) group member while it was in the process of joining the VSD (or RTO) group.</td>
</tr>
<tr>
<td>Master</td>
<td>the number of Master devices.</td>
</tr>
<tr>
<td>Primary BackUp</td>
<td>the number of primary backup devices.</td>
</tr>
<tr>
<td>BackUp</td>
<td>the total number of backup devices.</td>
</tr>
<tr>
<td>Ineligible</td>
<td>Notes that an administrator purposefully assigned a device so that it cannot participate in the selecting a new master device.</td>
</tr>
<tr>
<td>InOperable</td>
<td>Notes that a VSD (or RTO) group device has an internal problem.</td>
</tr>
<tr>
<td>Master Conflict</td>
<td>the number of conflicts that occurred on the master device.</td>
</tr>
<tr>
<td>Primary Backup Conflict</td>
<td>the number of conflicts that occurred on the primary backups device.</td>
</tr>
<tr>
<td>Tx Heartbeat</td>
<td>the number of transmitted heartbeats on the devices.</td>
</tr>
<tr>
<td>Rx Heartbeat</td>
<td>the number of received heartbeats on the devices.</td>
</tr>
</tbody>
</table>
Viewing RTO Counter Details

Click the Counters tab to view specific information about your RTO counters. The following table describes the information that is available from the RTO counters view:

Table 58: RTO Counters Details

<table>
<thead>
<tr>
<th>Item</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>the device(s) that are associated with the RTO.</td>
</tr>
<tr>
<td>Member ID</td>
<td>the member identification associated with this RTO</td>
</tr>
<tr>
<td>Status</td>
<td>the current status of the RTO: Active or Down.</td>
</tr>
<tr>
<td>Direction</td>
<td>the direction of the RTO: In or Out.</td>
</tr>
<tr>
<td>Lost Heartbeat</td>
<td>the number of heartbeats not received from the RTOs peers.</td>
</tr>
<tr>
<td>Counter to Active</td>
<td>the number of times that the RTO was placed to “active”</td>
</tr>
<tr>
<td>Counter to Set</td>
<td>the number of times that the RTO was placed to “set”</td>
</tr>
<tr>
<td>Counter to Lost Peer</td>
<td>the number of times that the RTO was placed to Lost Peer.</td>
</tr>
<tr>
<td>Counter to Group Detach</td>
<td>the number of times that the RTO was placed to Group Detach.</td>
</tr>
</tbody>
</table>

Monitoring IDP Clusters

If you have implemented IDP clusters for the purpose of redundancy, you can use the IDP Clusters Monitor to get an at-a-glance status of your IDP sensors that are in “clusters.”

Figure 176: IDP Cluster Monitor
Table 59 describes all of the information available from the IDP Cluster Monitor:

Table 59: IDP Cluster Monitor

<table>
<thead>
<tr>
<th>Item</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the cluster.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the cluster as OK, Warning or Fail.</td>
</tr>
<tr>
<td>Domain</td>
<td>Domain in NetScreen-Security Manager in which the source IDP cluster is managed.</td>
</tr>
</tbody>
</table>

**Viewing IDP Cluster Summary Information**

Click on the IDP Cluster Monitor, to view a summary of the top-level information on all IDP clusters. From the IDP Cluster Summary, you can view the following details about a specific cluster:

- Key details describing the cluster (such as name, Status, Cluster ID)
- HA Mode

The following table describes all of the information that is available from the IDP Cluster summary:

Table 60: IDP Cluster Summary

<table>
<thead>
<tr>
<th>Item</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>Domain in NetScreen-Security Manager in which the source IDP cluster is managed.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the cluster.</td>
</tr>
<tr>
<td>Cluster ID</td>
<td>Number uniquely identifying a cluster on a given Ethernet segment (retrieved from all nodes)</td>
</tr>
<tr>
<td>HA Mode</td>
<td>Whether the Cluster is in Hot-standby of Load Sharing mode.</td>
</tr>
<tr>
<td>Total Members</td>
<td>Total number of IDP sensors that are associated with the cluster.</td>
</tr>
<tr>
<td>Heartbeat Interval</td>
<td>Time interval (in ms) between each heartbeat</td>
</tr>
<tr>
<td>Heartbeat Lost Threshold</td>
<td>Threshold level (number of heartbeat intervals) required to declare that a device in the cluster has gone down.</td>
</tr>
<tr>
<td>No. of OK Members</td>
<td>Number of cluster members that are in OK state.</td>
</tr>
<tr>
<td>No. of Failed Members</td>
<td>Number of cluster members that are in FAIL state.</td>
</tr>
<tr>
<td>No. of Initializing Member</td>
<td>Number of cluster members that are in INIT state.</td>
</tr>
<tr>
<td>Master</td>
<td>Name of the master node.</td>
</tr>
<tr>
<td>Backup Availability</td>
<td>Whether a backup is available in the event that the Master node goes down.</td>
</tr>
<tr>
<td>No. of Backup Members</td>
<td>Number of active backup devices.</td>
</tr>
</tbody>
</table>
Monitoring IDP Cluster Members

Click on any IDP cluster to view details of each member in the cluster.

Figure 177: IDP Cluster Members

The following table describes all of the information that is available from the IDP Cluster Member Monitor.

Table 61: IDP Cluster Member Monitor

<table>
<thead>
<tr>
<th>Item</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the Device</td>
</tr>
<tr>
<td>Domain</td>
<td>Domain in NetScreen-Security Manager in which the IDP cluster member is managed.</td>
</tr>
<tr>
<td>State</td>
<td>State of the device as either INIT, OK or FAIL.</td>
</tr>
<tr>
<td>Elapsed Time (since last state change)</td>
<td>Duration since the device last changed state.</td>
</tr>
</tbody>
</table>

Using The Realtime Monitor

The following examples describe typical use cases for monitoring your security devices, VPNs, and NSRP clusters in NetScreen-Security Manager.

EXAMPLE: MONITORING DEVICE STATUS
In this example, you are a network administrator responsible for monitoring the day-to-day operation of all the security devices managed in your network. You are using NetScreen-Security Manager to manage your network, and Realtime Monitor to monitor the up/down connection status of all your security devices.
One day, you notice that the Connection Status on a mission-critical security device indicates that the security device is DOWN. You wait several minutes to verify that the connection status doesn’t resolve itself as intermittent network problems may cause a security device to temporarily indicate as DOWN. The Device Monitor still indicates that the security device is DOWN.

You next try to ping the security device. If you are successful in reaching the device, you can send a \texttt{get status} command to check the status of the security device.

If you cannot ping the security device, you will want to investigate further what may be a potential problem with the security device or your network. You next scan the Log Viewer for the log entry indicating that the security device has disconnected. You can filter the log entries in the Log Viewer to display only the log entries generated for the security device during the immediate time period that it went down. Viewing these log entries will also provide you with a context around the events leading to the security device disconnecting. This will help you to determine the cause of the problem.

You notice several very suspicious log entries that indicate that this security device may have been the target of an attack. You flag the log entries using the predefined flag types in the Log Viewer, and assign them to your security experts for further investigation.

\section*{Monitoring the Management System}

Use the Server Manager to access, monitor, and configure the NetScreen-Security Manager management system. The management system consists of a GUI Server and Device Server. Refer to the NetScreen-Security Manager Installer’s Guide for more information about the GUI Server and Device Server.

Security Manager contains the following:

- Servers
- Server Monitor

\section*{Configuring Servers}

Use Servers to add, configure and view key information about the GUI Server and Device Server:

\begin{table}[h]
\centering
\begin{tabular}{|l|l|}
\hline
\textbf{Indicator} & \textbf{Displays}... \\
\hline
Name & Name of the GUI Server or Device Server. \\
\hline
Server Type & whether the current server is a GUI Server, GUI Server Cluster, Device Server, or Device Server Cluster. \\
\hline
IP Address & IP address of the server. \\
\hline
Device Server Manager Port & the port open on the Device Server for security devices running ScreenOS 5.x. (Read Only) \\
\hline
\end{tabular}
\end{table}
Configuring Device Servers

You can also add and configure a Device Server. You might need to configure a Device Server when installing the GUI Server and Device Server on separate servers, or when installing the management system with High Availability (HA) enabled.

You can configure the following parameters on a Device Server:

- **Name**—you can give the Device Server any name you wish
- **IP Address**—IP address of the Device Server.
- **Server Type**—either Device Server or Device Server Cluster. If you are installing the management system with HA enabled, you need to configure the Device Server as part of an HA Cluster. After you specify that a Device Server will act as a Device Server Cluster, you can access additional tabs allowing you to further configure cluster details including the IP Address and port number of the secondary server, and e-mail notification.
- **Device Server Manager Port**—the port is set to 7800 by default. This field is READ only.
- **Device Server ID**—this is a unique ID assigned by NetScreen-Security Manager to each Device Server.
- **Mapped IP Address (if applicable)**—you can define multiple mapped IP addresses.
- **Device Polling**—the Device Server polls security devices it manages for Device, VPN, NSRP, or Interface statistics every 300 seconds by default. If you wish to change this behavior, you can edit the interval, using the Device Polling tab.
- **High Availability (HA)**—in order to configure a secondary Device Server, you need to specify the IP Address and port, and Mapped IP Address (if applicable).
- **Email Notification**—you can configure an SMTP server to send you an email notifying you of various events on the Device Server.

**NOTE:** You must restart the GUI Server to apply any changes that you have made.

Refer to the NetScreen-Security Manager Installer’s Guide for more information on adding and configuring the Device Server.

Configuring the GUI Server

You can configure the following parameters for the GUI Server:

- **Server Type**—Select GUI Server or GUI Server Cluster. If you are installing the management system with HA enabled, you need to configure the GUI Server as part of an HA Cluster.
- **IP Address**
- **HA parameters**
Email Notification—you can configure an SMTP server to send you an email notifying you of various events on the GUI Server. (See “Sending Email Notification of Downed Device” on page 639 for details.)

NOTE: You must restart the GUI Server to apply any changes that you have made.

Using Server Monitor

You can use the Server Monitor to view the status of the running GUI Server and Device Server. The Server Monitor lists all GUI Servers and Device Servers in your management system. For example, if you have installed a primary and secondary GUI Server in a high availability configuration, you could use the Server Monitor to monitor which GUI Server is currently active.

The Server Monitor provides two categories of information:

- Server status—displays information about the GUI Server or Device Server’s status, CPU, and memory. You can also choose to view the status of each server in the Server Monitor, or view additional server status details in a separate dialog box.

- Process status—displays information about the individual processes on a GUI Server or Device Server.

Viewing Server Status

To view the status of any server in the management system, select Server Manager in the navigation tree, and then select Server Monitor, as shown below:

Figure 178: Server Monitor

<table>
<thead>
<tr>
<th>Server Monitor (Machine-wide Info)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Server</td>
</tr>
<tr>
<td>Name</td>
</tr>
<tr>
<td>------</td>
</tr>
<tr>
<td>server_1</td>
</tr>
</tbody>
</table>

The following table lists and describes the columns that appear in the Server Monitor:

Table 63: Server Monitor Data

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the GUI Server or Device Server.</td>
</tr>
<tr>
<td>Server Type</td>
<td>whether the current server is a GUI Server, GUI Server Cluster, Device Server, or Device Server Cluster.</td>
</tr>
</tbody>
</table>
Chapter 12: Realtime Monitoring

You can sort data in the Server Monitor according to any column header by clicking that column.

Viewing Additional Server Status Details

If you are interested in monitoring additional details about your server’s status, you can view the Server Detail Status window by double-clicking any of the servers that appear in the Server Monitor. You can also right-click anywhere on the Server Monitor and select View Details. The Server Detail Status dialog box appears.
The following table describes information available in the Server Detail Status:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS</td>
<td>Operating system running on server machine.</td>
</tr>
<tr>
<td>Type</td>
<td>The server’s machine processor type.</td>
</tr>
<tr>
<td>CPU Idle</td>
<td>Percentage of the time the CPU was idle.</td>
</tr>
<tr>
<td>CPU User</td>
<td>Percentage of CPU utilization that occurred while executing at the user level.</td>
</tr>
<tr>
<td>CPU Kernel</td>
<td>Percentage of CPU utilization that occurred while executing at the system level.</td>
</tr>
<tr>
<td>CPU Usage</td>
<td>Percentage of CPU utilization.</td>
</tr>
<tr>
<td>1 Min Load</td>
<td>One minute load average.</td>
</tr>
<tr>
<td>5 Min Load</td>
<td>Five minute load average.</td>
</tr>
<tr>
<td>15 Min Load</td>
<td>Fifteen minute load average.</td>
</tr>
<tr>
<td>Total Mem</td>
<td>Total amount (in megabytes or gigabytes) of memory.</td>
</tr>
<tr>
<td>Used Mem</td>
<td>Amount (in megabytes or gigabytes) of used memory.</td>
</tr>
<tr>
<td>Mem Usage</td>
<td></td>
</tr>
<tr>
<td>Total Swap</td>
<td></td>
</tr>
<tr>
<td>Used Swap</td>
<td></td>
</tr>
<tr>
<td>Swap Usage</td>
<td></td>
</tr>
</tbody>
</table>

Figure 179: Viewing Device Server Details
Chapter 12: Realtime Monitoring

Viewing Process Status

From the Server Monitor, you can also view the status of all running server processes on the GUI Server or Device Server. This view is useful for troubleshooting purposes. If you are having problems with the server, you can quickly identify if a specific process on the server is the source of that problem.

To view process status, select Server Manager in the navigation tree, and then select Server Monitor. Double click the Server Monitor or click the node to expand the navigation tree. You can also right-click the Server Monitor to open it in a new window. Click to select a server to view the status of the processes running on it.

The following graphic depicts process status for the Device Server.

Figure 180: Process Status for the Device Server

<table>
<thead>
<tr>
<th>Name</th>
<th>Status</th>
<th>Total Mem Used</th>
<th>Phys. Mem Used</th>
<th>CPU Usage</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>.devSvrDataCollector</td>
<td>Up</td>
<td>670 MB</td>
<td>19 MB</td>
<td>0%</td>
<td>Version NSM 2</td>
</tr>
<tr>
<td>.devSvrDirectiveHandler</td>
<td>Up</td>
<td>691 MB</td>
<td>8 MB</td>
<td>0%</td>
<td>Version NSM 2</td>
</tr>
<tr>
<td>.devSvrLogFile</td>
<td>Up</td>
<td>5 MB</td>
<td>3 MB</td>
<td>0%</td>
<td>v1.3.1 (build LG)</td>
</tr>
<tr>
<td>.devSvrManager</td>
<td>Up</td>
<td>16 MB</td>
<td>4 MB</td>
<td>0%</td>
<td>v1.3.1 (build LG)</td>
</tr>
<tr>
<td>.devSvrStatusMonitor</td>
<td>Up</td>
<td>5 MB</td>
<td>3 MB</td>
<td>2%</td>
<td>v1.3.1 (build LG)</td>
</tr>
</tbody>
</table>

The following figure depicts process status for the GUI Server.

Figure 181: Process Status for the GUI Server

<table>
<thead>
<tr>
<th>Name</th>
<th>Status</th>
<th>Total Mem Used</th>
<th>Phys. Mem Used</th>
<th>CPU Usage</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>.guiSvrDirectiveHandler</td>
<td>Up</td>
<td>650 MB</td>
<td>15 MB</td>
<td>0%</td>
<td>Version NSM 20</td>
</tr>
<tr>
<td>.guiSvrManager</td>
<td>Up</td>
<td>58 MB</td>
<td>46 MB</td>
<td>0%</td>
<td>v1.3.1 (build LG)</td>
</tr>
<tr>
<td>.guiSvrMasterController</td>
<td>Up</td>
<td>649 MB</td>
<td>7 MB</td>
<td>0%</td>
<td>Version NSM 20</td>
</tr>
<tr>
<td>.guiSvrStatusMonitor</td>
<td>Up</td>
<td>5 MB</td>
<td>3 MB</td>
<td>2%</td>
<td>v1.3.1 (build LG)</td>
</tr>
</tbody>
</table>

Table 65 lists and describes the information that appears in the Process Status:
Table 65: Process Status

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the GUI Server or Device Server process.</td>
</tr>
<tr>
<td>Status</td>
<td>Displays if the process is Up or Down.</td>
</tr>
<tr>
<td>Total Mem Used</td>
<td>Total amount (in megabytes) of memory utilized.</td>
</tr>
<tr>
<td>Phys Mem Used</td>
<td>Total amount (in megabytes) of physical memory utilized.</td>
</tr>
<tr>
<td>CPU Usage</td>
<td>Percentage of CPU utilized.</td>
</tr>
<tr>
<td>Version</td>
<td>Process version.</td>
</tr>
</tbody>
</table>

You can sort server monitor data according to any column header by clicking that column.

**Using Management System Utilities**

Lists and describes utilities that you can use.

Table 66: Management System Utilities

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>logcount.sh</td>
<td>Provides information on peak/average logging rate, total log db size and average log size. This utility is located on the Device Server at: /usr/netscreen/DevSvr/utils</td>
</tr>
<tr>
<td>setSrsDbParams.sh</td>
<td>Configures the GUI Server for connection to the Statistical Report Server. This utility is located on the GUI Server at: /usr/netscreen/GuiSvr/utils</td>
</tr>
</tbody>
</table>
### Tech Support Utility

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tech-support.sh</td>
<td>Collects and compresses technical support data. This utility is located in</td>
</tr>
<tr>
<td></td>
<td>the utils directory on both the Device Server and GUI Server.</td>
</tr>
<tr>
<td>xdbAuditLogConverter.sh</td>
<td>Exports Audit Log data to a csv file or Syslog server.</td>
</tr>
</tbody>
</table>

**CSV Command Usage:**

For csv file, issue the following command:

```
./xdbAuditLogConverter.sh <xdb root> csv [csv full file path]
```

For example,

```
./xdbAuditLogConverter.sh /usr/netscreen/GuiSvr/var/xdb csv /tmp/audit.csv
```

This creates a file called audit.csv in the /tmp directory with audit logs in csv format. If the csv file path is not specified, audit logs in csv format are written to a default file called auditlog.csv in the current directory.

**Syslog Command Usage:**

For exporting data to a Syslog server, issue the following command:

```
./xdbAuditLogConverter.sh <xdb root> syslog [remote IP Address]
```

For example,

```
./xdbAuditLogConverter.sh /usr/netscreen/GuiSvr/var/xdb syslog 172.23.9.94
```

If you want to syslog to the host machine on which you are running this command, do not specify an IP address. For example:

```
./xdbAuditLogConverter.sh /usr/netscreen/GuiSvr/var/xdb syslog
```
Chapter 13
Analyzing Your Network

The Profiler is a network-analysis tool that helps you learn about your internal network, enabling you to create effective Security Policies and minimize unnecessary log records. After you configure the Profiler, it automatically learns about your internal network and the elements that comprise it, including hosts, peers (which host is talking to which other host), ports (non-IP protocols, TCP/UDP ports, RPC programs), and Layer-7 data that uniquely identifies hosts, applications, commands, users, and filenames.

The Profiler is supported in all IDP modes and in HA configurations, and it queries and correlates information from multiple devices.

This chapter contains the following sections:

- About the Dashboard on page 562
- About the Profiler on page 562
- Setting Up the Profiler on page 563
- About Profiler Views on page 567
- Recommended Profiler Options on page 576
- Accessing Data in the Profiler DB on page 580
- About Security Explorer on page 580
- Using Security Explorer on page 584
About the Dashboard

Known targets and sources of attacks or suspected targets and sources of attacks can be added to source or destination watch lists. The Dashboard is a near-real time monitor of these watch lists and the top 10 attacks within the previous hour. The frequency of time that these lists are updated is at a rate ranging from 2 minutes (default rate) to 30 minutes and happens automatically once the refresh rate is configured.

Use the Dashboard to create and configure both a destination and a source watch list as well as to display device status. This feature is available by default to the System Administrator. Use the dashboard or the Watch List to add or modify known targets and sources of attacks or suspected targets and sources of attacks.

About the Profiler

To use the Profiler, you must first configure the networks and hosts on your internal network that you want to monitor. The device monitors traffic at the network and application levels. You can use this data to investigate and analyze potential problems in the network and to resolve security incidents.

During profiling, the device records network activity at Layer-3, Layer-4, and Layer-7 and stores this information in a searchable database called the Profiler DB. The device uses session creation, session teardown, and protocol contexts to generate this database which defines all unique activities occurring on your network. Unique activities include attempts, probes, and successful connections. The device logs normal events only once, and it logs all unique events as often as they occur. A normal event is an event that reoccurs frequently and does not change. A unique event is an event that is new, unexpected, or does not match the normal traffic patterns of your network.

Example: Unique Events

For example, you allow users to use a laptop to connect to the corporate network while working in a conference room.

- **Normal Event.** Wendy holds a meeting every Tuesday at 4:00pm in conference room A. Every meeting, she connects her laptop to the network and accesses documents on the primary fileserver. Because the same event occurs multiple times, the device logs the event once and includes a timestamp that indicates the first and last times Wendy accessed the network from conference room A.

- **Unique Event.** The device logs changes from normal activity as a unique event in the Profiler.

  - During one of Wendy’s Tuesday meetings, she discovers she needs a document that resides on an Engineering server. She connects to that server and downloads the needed files. Because this connection differs from her usual activity, the device logs it as a unique event and records the IP and MAC addresses for both Wendy’s laptop and the Engineering server.
The device also logs other unique qualifiers, such as user name, email address for each individual that participated in the connection. If Wendy is out sick and another person logs into her laptop to run the meeting, the device records the connection as a unique event because the user name has changed.

To see all normal and unique events on your network, you configure and start the Profiler on multiple devices. This enables the Profiler to aggregate and display a complete view of your internal network.

**NOTE:** Profiler DBs remain on individual devices even if the devices restart.

After your devices have starting profiling, you can begin to use the profiled data to:

- **Set a network baseline.** A baseline can help you track the servers and hosts on the network, as well as the protocols and services those components use to communicate. By immediately locating new components on your network, you can ensure that those components are protected (with a Security Policy) and that you can track their status (with the Profiler). For details, see “Configuring a Network Baseline”.

- **Update vulnerable systems.** The Profiler uses passive fingerprinting to provide you with an inventory of operating-system and software applications, their versions, and what components use them. As new versions or security updates are announced, you must first determine if your network is affected, locate the affected components, and patch as appropriate. For details, see “Keeping Your Network Current”.

- **Immediately locate the source of an internal worm or trojan.** The Profiler can show you exactly when the worm or trojan entered your network, how it was introduced, and which network components are infected. By filtering the profile data, you can quickly identify the source and contain the attack to minimize impact, then investigate and recover from any damage. For details, see “Stopping Worms and Trojans”.

- **Detect violations of your corporate security policy.** The Profiler can help you confirm suspected violations such as rogue servers running on the network. Most of the time, however, you do not know exactly what you are looking for on the network. In these cases, it is easier to specify exactly what should be on the network, then detect any traffic that violates that specification. To detect violations, you can use a special type of object, called a permitted object, to define what you should see on the network.

The following sections detail how to setup, configure, and use your profiled data as described previously.

**Setting Up the Profiler**

Using the Profiler involves the following steps:

- Configuring the Profiler to collect specific information about your internal network
Starting the Profiler to enable your device to begin collecting data

Customizing Profiler Preferences

You configure your device to collect specific information and compile it into the Profiler DB.

NOTE: Because devices collect data from network components on your internal network, it is helpful to create Network Objects to represent those components before you begin configuring the Profiler. Alternatively, you can create new Network Objects directly from the Profiler.

Configuring the Profiler

You configure the Profiler using the Profiler settings that are available on the device settings in the Device Manager. Using the Device Manager, double-click to access a device managed in NetScreen-Security Manager, and click on Profiler Settings.

The Profile Configuration dialog box appears with the General tab selected. After selecting the device you want to use for profiling, you can then configure how that device collects data from your internal network.

Table 67 lists and describes the Profiler settings that you can configure from the General tab:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Application Profiling</td>
<td>Enables the Profiler to collect and track application data.</td>
</tr>
<tr>
<td>Include Probe and Attempt</td>
<td>Enables the Profiler to collect and track specific probes and attempts.</td>
</tr>
<tr>
<td>Include Non-tracked IP Profiles</td>
<td>Enables the Profiler to collect and track data from external hosts.</td>
</tr>
<tr>
<td>db limit (in MB)</td>
<td>Maximum database size for the Profiler on each device. By default, the maximum database size is set to 3GB.</td>
</tr>
<tr>
<td>Enable OS Fingerprinting</td>
<td>Enables the Profiler to perform passive OS fingerprinting to determine the operating system of an end host.</td>
</tr>
<tr>
<td>Refresh Interval (in secs)</td>
<td>Time interval (in seconds) that the Profiler refreshes OS fingerprinting data every 3600 seconds (60 minutes).</td>
</tr>
</tbody>
</table>

Enabling OS Fingerprinting

OS Fingerprinting passively detects the operating system of an end-host by analyzing TCP handshake packets. To ensure that this works, you need to verify that OS Fingerprinting is first enabled on the profiled device. After you have configured the Profiler with the tracked hosts, contexts, you must update the device.

OS fingerprinting works only for packets that contain a full fledged TCP connection, that is the tcp connection should have a SYN, SYN/ACK and a FIN connection. OS fingerprinting only works for operating systems that are supported on the device. A list of the supported operating systems is available on the device in a file called fingerprints.set at the following location:
Chapter 13: Analyzing Your Network

Configuring Network Objects
The first part of configuring the Profiler is to tell the device which Network Objects you want the device to profile. When you start the Profiler, the device begins collecting data from the selected hosts.

In the Tracked Hosts tab, select the Network Objects that represent your internal hosts. The device collects detailed information about traffic that passes between internal hosts, and groups traffic that does not match an internal host in a special IP: 73.78.69.84. Communication between an internal host and an external host is recorded only once. For example, the device records internal host A communicating to www.yahoo.com and www.cnn.com as one entry in the Profiler DB.

You can select unlimited internal network objects.

You can also use the Exclude List tab, to select the Network Objects that represent internal hosts you do NOT want to include in IDP profiling. You might want to exclude a host from the Profiler if you selected a group of Network Objects in the Tracked Host tab but want to exclude specific members of that group.

Configuring Context Profiles
Next, determine which contexts you want the device to record. In the Contexts to Profile tab, the context list includes only the contexts that can clearly identify a host, a user and/or an application. Select contexts that the device profiles. When you start the Profiler, the device begins collecting data on traffic that matches the selected contexts.

Example: Selecting Contexts
To track FTP logins, usernames, and commands, select the FTP contexts in the Contexts to Profile tab. After the Profiler is started, the device begins collecting information about FTP logins, usernames, and commands, enabling you to quickly identify who is using FTP on your network and what they are doing over that protocol.

When you first configure the Profiler, select all contexts. This enables the device to collect data about every context on your network, giving you a complete view of your network traffic. Later, when you have analyzed your traffic, you can eliminate contexts that you know will not be used on your network.

Select Profile Context to include context information. If you clear Profile Context, IDP profile data only includes higher-level traffic data such as source, destination, and service. If you want Profiler information to include context values and network probes (for example, port scans), also configure the Profiler to “Include Probes and Attempts” in the General tab.
Configuring Alerts

Use the Alert tab to configure the Profiler to indicate the appearance of a new host, protocol, or port on your internal network. When you enable New Host Detected, New Protocol Detected, or New Port Detected, the device generates a specific log record, such as PROFILER_NEW_HOST, in the Profiler Logs section of the Log Viewer, when the device discovers a new host, protocol, or port.

If you are configuring the Profiler for the first time, do not enable the new host, protocol, or port alerts. As the Profiler runs, the device views all network components as new, which can generate unnecessary log records. After the Profiler has learned about your network and has established a baseline of network activity, you should reconfigure the device to record new hosts, protocols, or ports discovered on your internal network. For details, see “Configuring a Network Baseline”.

Enable the Database Limit Exceeded alert to indicate when you have reached the maximum limit of the database size. You can configure the maximum limit of the Profiler DB using the dbLimit parameter in the General tab of the Profiler Configuration dialog box. The default is 500 MB; the minimum-maximum range is 0-500 MB. After a device reaches this limit, it begins purging the database.

Example: Using Alerts

For example, a network host performs the normal connections required for Internet connectivity (SMTP, POP3, HTTP, and so on). The host becomes infected by a worm and begins making outbound connections on an arbitrary port. The device logs the unique event and generates PROFILER_NEW_PROTO and PROFILER_NEW_PORT log records. The system immediately emails these log records to the Security Administrator, who can investigate the worm and take action to contain it.

Repeat the configuration process for each device in your network. When you have configured all devices on your network, you are ready to start the Profiler.

Updating Profiler Settings

After you have finished configuring settings on the Profiler, you must update those settings on the device. You can do this in the Device Manager by right-clicking on the device and selecting Update Device. The Device Update Options window appears and prompts you to Restart IDP Profiler After Device Update. Click OK to confirm. A Job Information window appears indicating the status of the update. After this is finished, the device begins collecting data for the Profiler DB.

Starting the Profiler

To manually start the Profiler, use the Devices menu, and select IDP Profiler > Start Profiler. In the Start Profiler dialog box, select the devices you want to use for profiling, then click OK. Alternatively, you can right-click on any device from the Device Manager, and select IDP Profiler > Start Profiler.

NOTE: After you start the Profiler for a specific device, the Enable Application Profiler setting in the device is automatically enabled.
About Profiler Views

As your devices begin profiling your internal network, they gather information about your network hosts, their peers, ports, and Layer-7 data.

Stopping the Profiler

To manually stop the Profiler, use the Devices menu, and select **IDP Profiler > Stop Profiler**. In the **Stop Profiler** dialog box, select the appropriate devices, then click **OK**. Alternatively, you can right-click on any device from the Device Manager, and select **IDP Profiler > Stop Profiler**.

NOTE: After you stop the Profiler for a specific device, the Enable Application Profiler setting in the device is automatically disabled.

Customizing Profiler Preferences

Use the Profiler Settings under the Tools menu to configure the following preferences for the Profiler:

- **Purge Profiler Database if Size Exceeds** - NetScreen-Security Manager purges the profiler database size if it exceeds 4GB (4000 MB) by default.
- **Max Profiler Database Size After Purging** - If the database size exceeds its maximum limit, NetScreen-Security Manager purges the profiler database size until the size reaches 3GB (3000 MB) by default.
- **Profiler Query Timeout** (120 seconds or 2 minutes by default)
- **Hour of Day to Perform Database Optimization** (midnight GMT by default)

About Profiler Views

The Profiler includes three main views that you can use to analyze data about your profiled network:

- **Application Profiler**: Displays a snapshot of Layer-7 traffic on your internal network including source, destination, service context, and value. Use this view to analyze specific applications that are running on your network, their versions, and the values for each supported context.

- **Network Profiler**: Displays a high-level snapshot of static information (Layer-3, Layer-4, and RPC protocols, ports and program numbers) on your internal network along with the Source/Destination IP, and Source/Destination MAC and Organizationally Unique Identifier (OUI). Use this view to quickly see which hosts are communicating with other hosts, and what services are passing between them.
Violation Viewer: Similar to the Network Profiler, the Violation Viewer displays a high level snapshot of network traffic - Layer-3, Layer-4, and RPC protocols, ports and program numbers along with the corresponding Source/Destination IP, and Source/Destination MAC and OUI. The Violation Viewer, however, enables you to more effectively view content that does not match or is in violation of certain patterns that you can set in a shared object called a Permitted Object. You must configure Permitted Objects before data appears in this view.

About the Application Profiler

The Application Profiler view is a table of information, like the Log Viewer that enables you to view and analyze dynamic application (Layer-7) traffic within a specific context. By default, this view contains only the data collected during the configured time interval; additionally, if you select a specific device, the Profiler displays only the information gathered by that device.

Figure 182: Application Profiler View

Table 68 lists and describes the information that you can view using the Application Profiler View:

Table 68: Network Profiler Data

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Src IP</td>
<td>Source IP address of the traffic profiled.</td>
</tr>
<tr>
<td>Dst IP</td>
<td>Destination IP address of the traffic profiled.</td>
</tr>
<tr>
<td>Service</td>
<td>All services of traffic profiled.</td>
</tr>
<tr>
<td>Context</td>
<td>All contexts of traffic that the devices selected in the Device table recorded.</td>
</tr>
<tr>
<td>Value</td>
<td>When you select a context, the values that your devices recorded for a selected context.</td>
</tr>
</tbody>
</table>
The Network Profiler view is another table of information, like the Log Viewer that enables you to view and analyze data related to static traffic (Layer-3, Layer-4, and RPC protocols, ports and program numbers) within the context of data corresponding to peer, host, and operating system.

Table 68: Network Profiler Data

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Src MAC</td>
<td>Source MAC addresses of traffic profiled.</td>
</tr>
<tr>
<td>Dst MAC</td>
<td>Destination MAC addresses of traffic profiled.</td>
</tr>
<tr>
<td>Src OUI</td>
<td>Source OUIs of traffic profiled. Note: OUI stands for Organizationally Unique Identifier. This value is a mapping of the first three bytes of the MAC address and the organization that owns the block of MACs. You can obtain a list of OUIs at <a href="http://standards.ieee.org/regauth/oui/oui.txt">http://standards.ieee.org/regauth/oui/oui.txt</a>.</td>
</tr>
<tr>
<td>Dst OUI</td>
<td>Destination OUIs of traffic profiled.</td>
</tr>
<tr>
<td>Src OS Name</td>
<td>Operating-system version running on the source IP of the traffic profiled.</td>
</tr>
<tr>
<td>Dst OS Name</td>
<td>Operating-system version running on the destination IP of the traffic profiled.</td>
</tr>
<tr>
<td>Hits</td>
<td>Number of occurrences that match the traffic profiled.</td>
</tr>
<tr>
<td>First Time</td>
<td>Timestamp for the first time the device logged the event (within the specified time interval).</td>
</tr>
<tr>
<td>Last Time</td>
<td>Timestamp for the last time the device logged the event (within the specified time interval).</td>
</tr>
<tr>
<td>Domain</td>
<td>Domain in which the device is managed in NetScreen-Security Manager.</td>
</tr>
<tr>
<td>Device</td>
<td>Device that profiled the data displayed.</td>
</tr>
</tbody>
</table>

About the Network Profiler

The Network Profiler view is another table of information, like the Log Viewer that enables you to view and analyze data related to static traffic (Layer-3, Layer-4, and RPC protocols, ports and program numbers) within the context of data corresponding to peer, host, and operating system.

Figure 183: Network Profiler View

Table 69: Network Profiler Data

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Src IP</td>
<td>Source IP address of the traffic profiled.</td>
</tr>
<tr>
<td>Dst IP</td>
<td>Destination IP address of the traffic profiled.</td>
</tr>
</tbody>
</table>
The Violation Viewer is very similar to the Network Profiler view. It displays all the same data that you can view in the Network Profiler view, but only for those object entries that do not match specific address and service criteria. By creating specific “permitted” objects, you can configure the Violation Viewer to display only those items that violate the criteria that you set.
Configuring Permitted Objects

Permitted Objects are shared objects specific to the Profiler. They enable you to configure objects in the Profiler containing simple rules, consisting only of source IP, destination IP, and service. The implied action is “permit”. You can then use the object to define what you should see on the network—as opposed to an attack object, which defines what you do not want to see as a set of rules. After you have created your permitted objects, the Violation Viewer displays all traffic that does not match the criteria that you have configured in these objects.

Example: Using the Violation Viewer to Detect Traffic That Uses Nonstandard Ports

The Profiler can help you confirm suspected violations such as SQL servers running on the network. Most of the time, however, you do not know exactly what you are looking for on the network. In these cases, it is easier to specify exactly what should be on the network, then detect any traffic that violates that specification.

For example, you want to detect internal traffic that uses a nonstandard port for its service.

1. From the Violation Viewer, click on the + icon that appears on the top of the right-hand window. You can also right-click anywhere in the right-hand window and select Add. A New Permitted Object window appears.
2. Name the object “Non-Standard -Ports”.
3. Right-click on the Service column and select Add Service.
4. Select all predefined services.
5. Click OK to save the permitted object. After you have created and saved the permitted object, the object automatically becomes available in the Profiler.
6. In the Profiler, select the Violation Viewer. In the Violation Viewer, select the new permitted object “Non-Standard-Ports”. The Profiler uses the object to filter the data collected from the devices. Traffic that matches the object (uses a standard service port) is filtered out, leaving only the traffic that does not match (uses a non standard service port).

You can now review the data in the Violation data viewer to see all traffic on your network that uses non standard service ports.

Now that you can see the traffic you do not want on your network, take the appropriate security measures, such as remove the unauthorized network components, incorporate the components/services into your existing corporate security policy, or create rules in your Security Policy to restrict the traffic to specific network components.

Example: Detecting Traffic That Is Not Using Primary Services
For example, you want to detect internal traffic that is not using the primary services for Web access, email, ping, and DNS services. In the Object editor, create a Permitted Object to permit all traffic that uses a standard service port. For Service, select the following predefined services:

- dns
- http
- https
- ping
- pop3
- smtp
- ssh

After you have created and saved the permitted object, the object automatically becomes available in the Profiler.

1. In the Profiler, select the Violation Viewer. Select the permitted object Internal Services. The Profiler uses the permitted object to filter the data collected from the devices. Traffic that matches the object (uses a service specified in the object) is filtered out, leaving only the traffic that does not match (does not use a service specified in the object).

2. Take appropriate measures to secure the network, such as:

- Investigate the source IP of the traffic and contact the user. If the traffic is legitimate, you might need to add the service to your corporate security policy to allow it on your network. You should also edit the permitted object to include the service so you no longer see the service in the Violation view.

- Create a rule in your Security Policy that drops connections between your internal network objects if the traffic uses a service that you do not allow on your network.

**Using Profiler Views**

You can perform all of the following functions within the Profiler views:

- “Filtering and Sorting”
- “Refreshing Profiler Data”
- “Viewing DB Information”
- “Viewing Detailed Network Information”
- “Purging the Database”
Filtering and Sorting

To help you view and analyze data in the Profiler, you can use criteria to filter information for each cell or column that appears in the Profiler.

Double-click in any of the columns that appear in the Filter Criteria. A dialog box appears enabling you to add entries that match the column you selected as criteria to filter the Profiler view on. The Profiler view automatically updates displaying the data that matches the criteria that you have set in the filter. You can also right-click on any entry in the Profiler view and select Add to Filter to add that entry as a filter criteria. Similarly, you can use the Remove From Filter option to remove that entry as a filter criteria.

Click on the Negate option to not display entries that match the criteria that you have set as a filter. You can also right-click on any entry in the Profiler view and select Toggle Filter Negation to not display entries that match that criteria.

Right-click on any filter criteria or on any entry in the Profiler view and select Clear Column Filter to disable filtering on entries that match the criteria set.

Right-click on any filter criteria or on any entry in the Profiler view and select Clear All Column Filters to disable all filtering.

Other options that you can set in the Profiler views include:

- **Sorting** - Click the column header, to sort columns in ascending or descending order.
- **Rearranging Columns** - Click a column header and drag it to a new position in the table to rearrange the order of the columns in the viewer.

All filter criteria are saved each time you logout of the UI.

**Example: Setting a Time Interval**

Profiler queries that return a very large amount of data may not complete in an acceptable amount of time. By default, queries that take longer than 120 seconds (2 minutes) will timeout by default.

In this case, the Profiler returns only that data that it has fetched in that amount of time. If this occurs, it is recommended that you refine your filter criteria. For example, if you want to analyze a specific event in your internal network, it is recommended that you set a time interval for the data.

The Profiler records the first-seen and last-seen timestamps for each entry in the database. You can set a time interval based on these timestamps. You can set an exact From and To time, or enter the Last day, hour, minute, or seconds:

- Use the **First Seen** setting to define a start timestamp threshold. If the device logged an event for the first time, and the event timestamp is after the start timestamp, the event displays in the Profiler view. For example, to see all new events in the last 2 days, configure the First Seen timestamp as the last 2 days.
Use the **Last Seen** to define a last timestamp threshold. If the device logged an event, and the event timestamp is before the last timestamp, the event displays in the Profiler view. For example, to see what network components have been idle over the last 10 days, configure the Last Seen timestamp as the last 10 days.

After you have configured a time interval, the selected Profiler view automatically applies the time interval as a filter criteria.

**Refreshing Profiler Data**

NetScreen-Security Manager fetches data from each of the devices that you are profiling automatically. By default, data is fetched from three (3) devices concurrently. When the Device Server completes fetching data from 1 device, it begins the operation on the next available device.

**NOTE:** You can change the default behavior that the Profiler uses to fetch data by editing parameters in the Device Server configuration file. Refer to the NetScreen-Security Manager Installer Guide for more information.

Click on the **Refresh** icon periodically to refresh the Profiler view with the latest data available.

**Viewing DB Information**

Click on the **Show DB Information** icon to view specific details about the Profiler DB including the database size.

**Viewing Detailed Network Information**

Click on the **Show Detail Viewer** to access the Detailed Network Information view. This view displays details for selected IP addresses, enabling you to further investigate the details of a connection, such as a username for an account on a host, open ports, RPC services, and so on. You can also right-click on any entry in the Profiler view and select **Show Detail Viewer** to access the Detailed Network Information view for that entry.

Use the IP and MAC areas to select the IP and MAC addresses of each interface on the selected host. For hosts with multiple interfaces, select the MAC address for the interface you want to investigate.

Click on any of the tabs in right-hand window to view different types of information that your devices have recorded for the selected IP address and MAC address.
Table 70 lists and describes the information that you can view using the Detailed Network Information View:

Table 70: Detailed Network Information Data

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Details about the selected host IP, including:</td>
</tr>
<tr>
<td></td>
<td>▪ IP Address</td>
</tr>
<tr>
<td></td>
<td>▪ MAC Address</td>
</tr>
<tr>
<td></td>
<td>▪ OUI (Organizationally unique identifier), a mapping of the first three bytes of the MAC address and the organization that owns the block of MACs (to obtain a list of OUIs, see <a href="http://standards.ieee.org/regauth/oui/oui.txt">http://standards.ieee.org/regauth/oui/oui.txt</a>).</td>
</tr>
<tr>
<td></td>
<td>▪ VLAN tag (if applicable)</td>
</tr>
<tr>
<td></td>
<td>▪ First Seen date and time that the devices first recorded traffic on that interface</td>
</tr>
<tr>
<td></td>
<td>▪ Last Seen date and time that the devices last recorded traffic on that interface</td>
</tr>
<tr>
<td></td>
<td>The OUI value enables you to see immediately the vendor of the network interface card (NIC) that is generating the packets.</td>
</tr>
<tr>
<td>TCP Ports</td>
<td>Details about the outbound TCP ports on the selected host IP.</td>
</tr>
<tr>
<td>UDP Ports</td>
<td>Details about the outbound UDP ports on the selected host IP.</td>
</tr>
<tr>
<td>Layer-3 Protocols</td>
<td>Details about the outbound Layer-3 protocols (IP) on the selected host IP.</td>
</tr>
<tr>
<td>RPC Services</td>
<td>Details about the outbound RPC services on the selected host IP.</td>
</tr>
<tr>
<td>Profiles</td>
<td>Details about the contexts and values on the selected host IP. Use the context and value fields to identify:</td>
</tr>
<tr>
<td></td>
<td>▪ Software version of the application</td>
</tr>
<tr>
<td></td>
<td>▪ Username/password of an account on that host</td>
</tr>
<tr>
<td></td>
<td>▪ Computer name</td>
</tr>
<tr>
<td>Peers</td>
<td>Details about how the selected host IP communicates with other hosts, including:</td>
</tr>
<tr>
<td></td>
<td>▪ Source IP address of peer traffic</td>
</tr>
<tr>
<td></td>
<td>▪ Destination IP of peer traffic</td>
</tr>
<tr>
<td></td>
<td>▪ Hits (number of times the source IP communicated with the destination IP)</td>
</tr>
<tr>
<td></td>
<td>▪ First Access date and time that IDP first recorded the peer traffic</td>
</tr>
<tr>
<td></td>
<td>▪ Last Access date and time that IDP last recorded the peer traffic</td>
</tr>
<tr>
<td></td>
<td>If the source IP is the selected interface, you can use the destination IP address to identify all the hosts that the interface sent traffic to, both internal and external, as well as the number of times traffic was sent.</td>
</tr>
<tr>
<td>Summary</td>
<td>Lists all the details of the other View box selections in HTML format.</td>
</tr>
</tbody>
</table>

Purging the Database

When the Profiler DB reaches a maximum size (4 GB by default), it begins purging records (oldest first) automatically. The Profiler DB stops purging records when it reaches a certain set minimum size (3 GB by default). You can use the Profiler settings in the Tools preferences menu to change these parameters.
If you wish, you can manually purge the Profiler DB of all records by clicking **Clear All DB**. This operation may take up to 1 minute to complete. During this time, a tool tip message appears on all other connected UIs indicating that a Clear All DB operation is in progress. After the data clears, you can click on the **Refresh** icon to get new data.

### Recommended Profiler Options

The following are recommended for using the Profiler:

- Configuring a Network Baseline
- Keeping Your Network Current
- Proactively Updating Your Network
- Reacting to Vulnerability Announcements
- Stopping Worms and Trojans

### Configuring a Network Baseline

A baseline is a static view of your network traffic patterns. This view, which is compiled from multiple views of traffic over time, represents the normal, known activity that occurs on your network. By setting a baseline for your network, you can quickly detect any traffic that deviates or violates that baseline and take appropriate measures.

#### Identifying a Baseline

Your devices begin learning your network baseline as soon as the Profiler starts. As your devices profile the network for the first time each component appears as new. To avoid unnecessary log records generated by Profiler alerts, you should ensure that alerts are not enabled in the Alerts tab of the Profiler Configuration dialog box.

During the learning phase, your devices profile the network hosts, servers, and software applications that they protect; the Profiler synchronizes profile information from the devices and creates an initial view of your network. Each time you synchronize the devices, the Profiler incorporates any new data into this view, creating a more complete, up-to-date image of your network. You should continue to synchronize data daily until you feel the Profiler is accurately depicting your normal traffic patterns.

Remember, because all networks are different, the learning phase can range from a few hours to a few weeks.

#### Setting a Baseline

When you are satisfied that the Profiler has detected each host, protocol, and port that you want to profile, you have successfully created a network baseline. By itself, this baseline view can help you implement software/hardware upgrades, take inventory for new support contracts, plan for a network ROI investigation, and so on.
However, the true power of your network baseline is to enable your devices to identify network deviations. The Profiler uses the baseline to identify new or unknown hosts or software that might represent a network vulnerability. Network deviations can be a simple application update, or a serious security breach.

When enabled, if the device discovers a new host, protocol, or port, the device generates a log record, such as PROFILER_NEW_HOST, in the sub category column of the Log Viewer.

**Keeping Your Network Current**

Typical networks include multiple servers and hosts, each running different operating systems and software applications that are important to users on the network. While this variety helps users accomplish their tasks, it can make it difficult to keep your network systems current. As new versions or security updates are announced, you must first determine if your network is affected, locate the affected components, then patch as appropriate.

To help you maintain control of your network software versions, the Profiler uses passive application fingerprinting to identify the application version for each service used in your network. Additionally, your devices collect and store the user name and other important information for each application. These profiling activities provide you with an inventory of operating-system and software applications, versions, and the components that use them.

You can use this information to proactively update your network and/or respond quickly to vulnerability announcements.

**Proactively Updating Your Network**

To eliminate security holes, you should update your software applications regularly. Some guidelines:

- **Research known vulnerabilities.** Compare the information in the Profiler with a software vulnerability database, such as Security Focus at [http://www.securityfocus.com/bid](http://www.securityfocus.com/bid) or Common Vulnerabilities and Exposures (CVE) at [http://www.cve.mitre.org/cve/](http://www.cve.mitre.org/cve/).

- **Plan to patch.** After you identify your vulnerable systems, schedule a regular maintenance time to keep downtime and disruption to a minimum.

Even if your network components do not require security patches or updates, they might use default configurations. Many network device vendors use a common phrase, the vendor name, or other simple word as the default password for accessing the administration interface of their device. Because these passwords can be guessed easily, the vendor recommends that users change the default password immediately. However, for convenience, some users leave the default configuration password, unknowingly opening a security hole in the network. The Profiler captures user information that you can use to see who is logging in to network devices so you can verify that they are from trusted IP addresses.
Reacting to Vulnerability Announcements

New network attacks and exploits are discovered every day. When new security patches are issued, use the Profiler to quickly identify which systems are running the affected software version, then patch them appropriately.

For large networks, it is difficult to patch everything immediately. Plan your patching process by prioritizing based on the importance of the resources. Critical, high-risk, and heavily used resources should be patched first, while less important, minimally used resources might be able to wait.

Example: Identifying Vulnerable Components

For example, Microsoft announces a vulnerability in version 5.0 of the Microsoft Internet Informations Services (IIS). To quickly identify all network components running the vulnerable version:

1. Select the Application Viewer to see the applications running on the network.

2. In the Context Filter data table, select HTTP Header Servers. The value data table lists all Web servers currently running. As shown below, the network uses the following Web Servers:
   - Apache (two versions)
   - Microsoft IIS, version 5.0

3. Select the Microsoft IIS 5.0 value to find out which IP addresses are running the IIS server. The Application Data Viewer displays the destination IP address of the service, which is the IIS server.


Stopping Worms and Trojans

Worms and trojans often bypass firewalls and other traditional security measures to enter a network. Because worms and trojans operate inside a network, external firewalls might not be able to detect them.

Use the Profiler to determine when a worm or trojan entered your network, how it was introduced, and which network components were infected. By filtering the profile data you can identify the source and contain the attack to minimize impact, before investigating and recovering from any damage.

Example: SQL Worm

For example, your corporate security policy does not permit SQL servers on the internal network. However, during a regular Microsoft update, SQL applications are installed on a network server, without your knowledge. Because you are not aware that an SQL server is running on your network, you do not attempt to block SQL attacks at your firewall or IDP system. Suddenly, the SQL Slammer worm attacks and infects your network.

Using the Profiler:
1. Create a custom TCP service object to represent Microsoft SQL (default port: TCP/1433).

2. Restart the Profiler.

3. Select the Network Profiler to quickly see the source, destination, and service of traffic on your network.

4. In the Service data table, select the SQL service you just created. The Network data viewer lists all network components current running SQL servers.

5. Take appropriate measures to secure the network, such as:

6. Apply patches.
   - Remove the components from your network.
   - Remove SQL from all components.
   - Create a rule in your Security Policy that drops all SQL connections between your internal network objects.

For example, the Blaster worm uses a special ICMP (ping) packet to exploit a vulnerability in Remote Procedure Call (RPC), a Microsoft networking tool that enables desktops to share files over a remote network. Your corporate firewall denies RPC filesharing traffic to protect sensitive corporate files from Internet users, but enables RPC filesharing on a local network for convenience.

Example: Blaster Worm
A laptop user uses a wireless network to access the Internet. Because the laptop is configured to allow RPC, it contracts the Blaster worm from an infected user on that network. When the user return to the office and connects the laptop to the corporate network, the worm immediately begins scanning the internal network and infecting all components that have RPC enabled.

Because the Profiler records all unique activity on the network, it identifies the ICMP packet scans as a new event. Because you have configured the Profiler to send alerts for new hosts, you also receive a log record on your pager indicating that a new host has joined the network. A quick check of the Profiler’s Network view tells you that the new event is a user laptop suddenly scanning the entire network using ICMP, a possible sign of the Blaster worm.

Using the Profiler:
1. Restart the Profiler.

2. Select the Network Profiler to quickly see the source, destination, and service of traffic on your network.

3. In the Service data table, select the ICMP service. The Network data viewer displays all network components using ICMP.
4. In the Access data table, select probe. The Network data viewer displays all network components that used ICMP to probe the network.

5. Set a Last Seen time interval of two hours.

The Network data viewer displays all network components that used ICMP to probe the network in the last two hours. You can now see that one IP address, 192.168.4.66, is currently probing your network using ICMP. However, because you use DHCP to dynamically assign IP addresses, you need to identify which user laptop is currently using that IP address.

6. In the Network Profiler, select the source address you want to investigate. The MAC/View area displays the host detail for the IP address.

7. In the View menu, select Profiles. The MAC/View area displays the context/value information about the IP/Mac address.

The IP/MAC address has the unique asset tag "darkness." After checking your IT inventory, you determine who the laptop user is and patch the infected system.

Accessing Data in the Profiler DB

The Profiler DB is located on the NetScreen-Security Manager GUI Server.

To query on the actual records in the database:

Log into the GUI Server as the PostgreSQL user. By default, the PostgreSQL user is set to "netscreen".

Navigate to the directory where the Profiler DB is located (/usr/local/nsmpsql/bin).

Run any PostgreSQL command. For example, you can type the following command:

```bash
./psql -d profilerDb
```

About Security Explorer

The Security Explorer is a powerful, graphical tool that enables you to visualize and correlate network behavior based on data collected in the Profiler, Log Viewer and Report Manager. You can use the Security Explorer to:

- Get a dynamic, interactive view of your network
- Drill down on a particular host or server and view all the different attacks, open ports, destination or peer IP addresses
- Move easily between hosts and peers and trace a connection or attack
- Toggle easily between different views or slices of the network, as well as be able to explore the contextual information (logs, reports, IDP attacks, IP addresses, etc) within the SE pane
The main component is a graph that represents the relationships between data objects, such as hosts, services, attacks, etc.

There are five main views in the Security Explorer:

- Security Explorer Main Graph
- Connections Detail Pane
- Reference Point Pane
- Log Viewer
- Reports Viewer

Figure 184: Security Explorer

Security Explorer Main Graph

The main component of Security Explorer is a visual graph that displays the following nodes:

- Host - displayed as an IP address
- Network - displayed using CIDR notation (ip/class: 8/16/24)
- Protocol - these include TCP, ICMP etc
- Attack - specific attack object name
Service - displayed in protocol/port notation

Service range - displayed in protocol/port range notation, e.g. TCP/1-1024

Context - plain text describing one protocol attribute, e.g. 'SSL server version'

Value - value specific for a context e.g. for 'SSL server version' the value '3.1'

Graph Types

Depending on the starting reference point, the following graphs appear in Security Explorer depicting relationships between objects (i.e., peers of a host or services for a host):

- **Peer IP** - displays selected host and all peers of this host. Hosts are grouped in networks /8, /16, /24. Every network appears as a graph node and is connected to its sub-networks and hosts.

- **Outbound Services** - displays a host or network and its outbound services. The services are grouped by protocol (TCP, ICMP, etc.) and by service port range. Every group is displayed as a separate node, e.g. for a host 10.150.151.3 with outbound service FTP the graph structure is: [Host:10.150.151.3]- [Protocol:TCP]- [Service range:TCP/0-1024]-[Service:TCP/21]

- **Inbound Services** - displays a host or network and its inbound services. The services are grouped by protocol (TCP, ICMP, etc.) and by service port range. Every group is displayed as a separate node, e.g. for a host 10.150.151.3 with outbound service FTP the graph structure is: [Host:10.150.151.3]- [Protocol:TCP]- [Service range:TCP/0-1024]-[Service:TCP/21]

- **Server Profiles** - displays one host or network and the context for server-related traffic. Every context is connected to its host/network related value e.g. on a host is an SSL server in the version 3.1 running. The graph displays the host and its relationship to the host connected 'SSL Server Version' context and to the context connected value '3.1'.

- **Client Profiles** - displays one host or network and context for the client related traffic. Every context is connected to its host/network related value e.g. on a host is a SSL server in the version 3.1 running. The graph displays the host and its relationship to the host connected ‘SSL Server Version’ context and to the context connected value '3.1'.

- **Outbound IP** - displays all outbound hosts/networks for a selected service, context or value.

- **Inbound IP** - displays all inbound hosts/networks for a selected service, context or value.

- **Value** - displays all values for a selected context.

- **Network-Attack** - displays attacks for one selected network/host

- **Attack-Network** - displays one attack and source/destinations IPs or ports where the attack appears.
Connections Detail Pane

Use the Connection Details pane to view a list of all objects connected to the currently selected object in the graph. For example, if you are viewing an Outbound Services graph, and a host is selected, the Connections Detail pane contains all services for this host. If a Peer IP graph appears, the Connections Detail pane contains all peers for the selected object.

Double clicking on one of the objects in the Details pane displays the relationship graph for it.

Reference Point Pane

Use the Reference Point pane to view a list of reference objects. Next to the graph, a list of the possible initial objects appears:

- Address objects - for host/network selection. The selected host appears in a Peer Graph, with selected network in a Outbound Service graph.
- Service objects - are displayed in an Outbound IP graph.
- Context objects - are displayed in a Value graph.
- IDP Attacks - are displayed in an Attack-Network graph.

Double-click on one of the objects to set it as a point of reference in the main graph.

Log Viewer

Use the Logs tab in the viewer that appears below the main graph to view all logs related to the point of reference that you have selected.

Reports Viewer

Use the Reports tab to generate and view one of the following reports in Security Explorer:

- Top Alarms
- Top Traffic Alarms
- Top Traffic Logs
- Top IDP/DI Attacks
- Top Screen Attacks
- Top Destination IP’s
- Critical severity attacks
- High severity attacks
- Attacks over time
- Attacks by severity
- Attacks by flag

Use the Source/Destination Address pull-down menu to view these reports based on either the Source IP or Destination IP.

Use the time duration pull-down menu to view data in these reports during a specific time frame. You can select to view data from the last 24, 12, 8, 4, 2, 1 hours.

Using Security Explorer

You can launch the Security Explorer in any of the following ways:

- From the Security Monitor tree node, select Security Explorer
- From the Log Viewer, for any anomaly, signature or custom log, right-click on a Source/Destination Address, Protocol/Destination Port, NAT Source/Destination Address and select Launch Security Explorer

NOTE: For all other log categories, the Launch Security Explorer option is not available.

- From the Profiler, right-click on a Source/Destination Address, Context or Service in any entry and select Launch Security Explorer

If you launch Security Explorer from the Security Monitor without any reference point, the main graph appears empty.

If you launch Security Explorer using a starting point of reference from the Log Viewer or Profiler, that reference point is depicted in the main graph.

Permissions

To use the Security Explorer, you must have the proper administrative privileges including the View Security Explorer activity. By default, all IDP administrators have this privilege. Depending on other activities you may want to use with Security Explorer, you also may need proper administrative privileges to:

- View Profiler
- View Device Logs
- View Historical Log Reports
- View Devices
- View Shared Objects

If you do not have proper permission to perform all activities, you may only have access to a reduced set of Security Explorer features. For example, if you do not have View Profiler privileges, you will not be able to view graphs related to the Profiler (i.e., Peer graph).
If an administrator is logged into the global domain, all devices in the address point of reference list appear. This includes all global and sub-domain objects. If an administrator is logged into a sub-domain, only those devices in the current sub-domain devices appear.

**Analyzing Relationships**

After you have established your main point of reference, a list of possible navigation options appears. Every option represents a transition from one graph to another.

**Viewing Data**

For your convenience, the following view options are available making it easier for you to view and analyze each node in the main graph:

- **Center Node** - Click on any node that appears in the main graph to center it. You can also right-click on the node and select Center Node.
- **Expand Node** - If you want to view all objects related to a specific node, right-click on any node and select Expand Node.
- **Collapse Node** - If you are not interested in viewing all objects related to a specific node, you can reduce extraneous data by right-clicking on any node and selecting Collapse Node.
- **Hide Node** - If you are not interested in viewing a specific node, and you want to remove it from viewing in the graph, right-click on any node and select Hide Node.
- Use the zoom in and zoom out icons to increase or decrease the size of the nodes on the graph.
- Use the back arrow to view the previous graph. Use the forward arrow to view the next graph.

**Transitioning to Other Relational Graphs**

Use the icons that appear in the main graph to quickly access additional information related to your point of reference. Depending upon the type of icon that you select, you can transition to another graph. The following table describes the graphs that you can transition to:

<table>
<thead>
<tr>
<th>Table 71: Transitional Graphs</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Node</strong></td>
</tr>
<tr>
<td>Host</td>
</tr>
<tr>
<td>Network</td>
</tr>
<tr>
<td>Service</td>
</tr>
<tr>
<td>Service range</td>
</tr>
<tr>
<td>Context</td>
</tr>
</tbody>
</table>
Setting a Time Duration
Click on the **Time Period** icon to set a specific time period during which you want to view data.

Viewing Predefined Reports
Use the Reports pull-down menu to view a predefined report of that data. There are three predefined reports that you can access:

- Top Attacks - displays the most common attacks on the network
- Top Attackers - displays most common origins of attacks on the network
- Top Targets - displays top destination targets of attacks on the network.

Refreshing Data
Click on the Refresh icon to update the Security Explorer with the latest data available.

Adding and Removing Panels
You can also view additional data and graphs by adding and removing additional panels to Security Explorer:

- Use the `+` icon to add a Security Explorer panel. The new panel appears as a new tab in the main graph area. Click on the tab to access the new panel
- Use the `-` icon to remove the current Security Explorer panel

**Exporting to HTML**
You can also export any data depicted in the Security Explorer to an HTML file by using the Export to HTML option.
Juniper Networks NetScreen-Security Manager integrates log information from multiple devices to help you access and distill data about the traffic on your network.

The Log Viewer presents log data as a log entry in a table; a log entry contains the details of the traffic that triggered the log, such as IP address, port number, and source and destination zones. This log data is also automatically used to generate predefined reports, helping you to interpret event information in a specific context. Or, to perform your own investigation, use the Log Investigator to view cross-tabulations between sources, destinations, subcategories, and destination ports.

The Audit Log Viewer presents log entries triggered by administrative changes (changes made to the NetScreen-Security Manager system). An audit log entry includes details about the administrative event, such as the administrator name, timestamp of the change, and job details.

You can configure each managed security device to generate and export specific log records to multiple formats and locations, such as syslog, xml, or email servers. You can also forward logs that meet specified criteria to predefined formats and locations.

This chapter contains the following sections:

- About Logging on page 588
- Configuring Logging on page 590
- Using the Log Viewer on page 601
- Using the Log Investigator on page 620
- Using the Audit Log Viewer on page 631
- Managing Log Volume on page 635
- Forwarding Logs on page 639
About Logging

Logging is the act of recording information about an event. In NetScreen-Security Manager, each event that occurs on your network or in your management system can be recorded and stored as a log entry. To view log entries from the NSM UI, you can use one or more of the logging-related UI components, such as the Log Viewer or the Log Investigator.

It may be helpful to visualize log entries being sent or pushed from the device to the NSM Device Server, which then pushes the log entries to the logging database. A UI module (the Log Viewer or Report Manager) requests or pulls the log entries in the logging database and displays the entries in the UI.

About Log Entries

A managed device generates a log entry when an event matches the configured logging conditions. The log entry, which contains details of the event, is sent to the NSM Device Server and stored in the logging database. You can view log entries in the NSM UI.

In a single log entry, you can view detailed information about where traffic comes from (the source address), where traffic goes (the destination address) and a description of the event that triggered the log entry. You can also view summarized information about events and alarms for multiple log entries. This data can help you analyze log entries and determine the effectiveness of your current Security Policies and device configurations.

About Log Events

Managed devices generate log entries based on events. Typically, devices generate log entries when:

- An event matches a rule in which logging is enabled. When you configure a rule for logging, the device creates a log entries for each event that matches that rule.
- An event matches a predefined set of conditions configured on a managed device or the management system.

Some events generate log entries that appear in the Log Viewer, while others appear in the Realtime Monitor. Table 72 details event-generated log entries.

<table>
<thead>
<tr>
<th>Events</th>
<th>Description</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack, Alarm, Other</td>
<td>Generates log entries for events related to network activity on the device that violates a set threshold.</td>
<td>Log Viewer</td>
</tr>
<tr>
<td>VPN Events</td>
<td>Generates log entries for events related to VPN tunnels. These log entries are used to produce statistical information for monitoring purposes.</td>
<td>Realtime Monitor &gt; VPN Monitor</td>
</tr>
</tbody>
</table>
Chapter 14: Logging

589

About Log Severity

The log severity level defines the urgency of the information contained in the log entry. The severity level of a log entry depends on the log category, such as information, traffic, or configuration log entries.

You can configure a managed device to generate log entries only for those events that meet a specific severity level criteria. Additionally, you can configure the device to forward log entries that contain a specific severity to a specific destination, such as a console location or syslog server. You can forward multiple log entries with different severity levels to the same log destination.

Juniper Networks assigns a predefined severity level in the firmware of each Juniper Networks security device. However, these severity levels are not the same as the severity levels that appear in the log entries viewed in a NetScreen-Security Manager UI module.

Table 73 details how NetScreen-Security Manager handles severity levels as defined by ScreenOS:

<table>
<thead>
<tr>
<th>Events</th>
<th>Description</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration, Information,</td>
<td>Generates log entries for events related to device configuration, NetScreen-Security Manager configuration, Security Policy rules, and traffic activity on the managed device.</td>
<td>Log Viewer</td>
</tr>
<tr>
<td>Self, Policy, Traffic</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flow, Ethernet, Attack,</td>
<td>Generates log entries for events related to packet flow, ethernet objects, network attacks, and Security Policy rules. These log entries are used to produce statistical information for monitoring purposes.</td>
<td>Realtime Monitor &gt; Device Monitor</td>
</tr>
<tr>
<td>Policy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protocol Distribution</td>
<td>Generates log entries for events related to protocols used in network activity. These log entries are used to produce statistical information for monitoring purposes.</td>
<td>Realtime Monitor &gt; Device Monitor</td>
</tr>
</tbody>
</table>

Table 73: Log Entry Severity Levels

<table>
<thead>
<tr>
<th>NetScreen-Security Manager Severity</th>
<th>ScreenOS Severity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>Emergency</td>
<td>Log entries triggered when traffic matches a critical severity attack object. Also includes log entries triggered by the SCREEN-level attacks, SYN attacks, Tear Drop attacks, and Ping of Death attacks.</td>
</tr>
<tr>
<td>Alert</td>
<td></td>
<td>Log entries triggered by the general firewall SCREEN-level attacks or other conditions that require immediate attention, such the expiration of license keys.</td>
</tr>
<tr>
<td>Major</td>
<td>Critical</td>
<td>Log entries triggered when traffic matches a major severity attack object. Also includes log entries triggered by changes in the device function, such as high availability (HA) status changes.</td>
</tr>
<tr>
<td>Minor</td>
<td>Error</td>
<td>Log entries triggered when traffic matches a minor severity attack object. Also includes log entries triggered by errors in device function, such as a failure in antivirus scanning or in communicating with SSH servers.</td>
</tr>
<tr>
<td>Warning</td>
<td>Warning</td>
<td>Log entries triggered when traffic matches a warning severity attack object. Also includes log entries triggered by questionable device activity, such as a failure to connect to email servers and authentication failures, timeouts, and successes.</td>
</tr>
</tbody>
</table>
Viewing Logs

NetScreen-Security Manager logging tools provide a high-level view of the activity on your network, enabling you to view summaries as well as detailed information. You can choose to view log entries for an event that occurs across domains (you must have the requisite permissions), as well as for specific device groups, clusters, firewalls, and so on.

Because you collect log entries from multiple devices, log analyzing, log volume, and log management are important concerns. To control the amount of log data displayed onscreen, use tools such as filters, flags, and custom views to help identify patterns, even isolate log entries from devices that appear to be the source of problems. For further investigation, use the Log Investigator tools to cross-tabulate source, destination, and attacks. Based on your analysis, you can then edit the rules in your Security Policies to modify how NetScreen-Security Manager handles your log entries.

NetScreen-Security Manager includes three primary logging modules:

- **Log Viewer**—Presents complete, summarized, or detailed log-entry information in a table format. You can view an individual log entry to analyze the raw log data, or use filters to view subset of log entries. You can also use column settings and flags to control how the UI presents log information. The Log Viewer displays each log entry as it enters the database in real-time, displaying its fields in the Log Viewer. For details, see “Using the Log Viewer” on page 601.

- **Log Investigator**—Enables you to correlate log data. The Log Investigator is an exploratory data analysis tool that cross-tabulates on two dimensions. Log entries are linked to the Log Viewer, helping you perform an interactive analysis. For details, see “Using the Log Investigator” on page 620.

- **Audit Log Viewer**—Tracks administrative changes made to a managed device by a NetScreen-Security Manager administrator. Log-entry details include the admin that performed the change, what time the change occurred, and the job results. For details, see “Using the Audit Log Viewer” on page 631.

Configuring Logging

Before your managed device can generate log entries or log data, you must configure your devices and the NetScreen-Security Manager system for logging. You can configure an individual device to generate attack, alarm, configuration, information, and self log entries for specific destinations.
Chapter 14: Logging

To view log entries and log data in the NetScreen-Security Manager UI, you must configure the individual device to generate log information for NetScreen-Security Manager, and enable one or more severity settings for NetScreen-Security Manager. However, you are not required to configure the settings for other destinations if you do not use those destinations for log management.

Configuring the Device for Logging

At the device level, you can configure how and where the device sends its log entries. For each destination, you can define:

- The category of log entries you want the device to generate and forward to a specific destination, and
- The severity of log entries you want the device to forward to a specific destination

The severity setting applies to all log types for that destination. For example, if traffic log entries are enabled for NetScreen-Security Manager, but the severity setting specifies critical and major severities, NetScreen-Security Manager receives only critical and major traffic logs; all other severity traffic log entries are generated, but never sent to the management system. Unsent traffic log entries are stored on the device and discarded when the device log storage capacity is exceeded.

Configuring Severity Settings

Use the General settings to select the severity levels of the log entries you want to forward to a specific location. Juniper Networks assigns a predefined severity level for each event that generates a log entry on a security device; using NetScreen-Security Manager, you can configure a device to send log entries with specific severity levels to specific destinations.

For each destination (except Firewall Options), you can specify one or more severity levels (for details on severity levels, see “About Log Severity” on page 589).

NOTE: Debug messages are sent only to syslog, and do not appear in any NetScreen-Security Manager UI module.

Not all destinations support all log entry severities. The following table details the log entry severities accepted by each destination (except Firewall Options):
Table 74: Destinations of Log Entry Severities

<table>
<thead>
<tr>
<th>Destination</th>
<th>Description</th>
<th>Severities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console</td>
<td>The PC you use to view log entries in NetScreen-Security Manager.</td>
<td>All severities</td>
</tr>
<tr>
<td>Email</td>
<td>An Email server to which you want log information forwarded.</td>
<td>Emergency, Alert, Critical, Notification</td>
</tr>
<tr>
<td>Syslog</td>
<td>The syslog facility on the Device Server.</td>
<td>All severities</td>
</tr>
<tr>
<td>WebTrends</td>
<td>A WebTrends server to which you want log entries forwarded.</td>
<td>All severities</td>
</tr>
<tr>
<td>NetScreen-Security Manager</td>
<td>The NetScreen-Security Manager server.</td>
<td>All severities</td>
</tr>
<tr>
<td>PCMCIA</td>
<td>A PCMCIA device to which you want log entries forwarded.</td>
<td>All severities</td>
</tr>
<tr>
<td>Internal</td>
<td>An destination within the current device to which you want log entries forwarded.</td>
<td>All severities</td>
</tr>
</tbody>
</table>

To select log entry severities for a destination, open a device configuration and select Report Settings > General, then select the destination.

**Forwarding Self Log Entries (Firewall Options)**

Self log entries display information on traffic that was dropped by the security device or on traffic that terminates on the device. Any packet that terminates at the device generates a self log entry; Telnet, Ping, BGP, and OSPF connections all terminate at the device, and can trigger a self log entry.

A self log includes the date and time a packet was dropped, the source address of the packet, the destination address of the packet, the duration for which the packet was active, and the service associated with the packet. You can disable or enable logging of dropped packets for specific traffic types, including ICMP, IKE, SNMP, and multicast packets.

To configure self log entries, open a device configuration and select Report Settings > General. Click the Firewall Options tab and configure the following settings:
Table 75: Self Log Entry Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log ICMP Packets to Self</td>
<td>Creates a log entry for an ICMP (ping) packet that was dropped or terminated at the device.</td>
</tr>
<tr>
<td>Log IKE Packets to Self</td>
<td>Creates a log entry for an IKE packet that was dropped or terminated at the device. When negotiating an IKE key, the VPN client communicates with the security device.</td>
</tr>
<tr>
<td>Log SNMP Packets to Self</td>
<td>Creates a log entry for an SNMP packet that was dropped or terminated at the device.</td>
</tr>
<tr>
<td>Log Multicast Packets to Self</td>
<td>Creates a log entry for a multicast packet that was dropped or terminated at the device.</td>
</tr>
</tbody>
</table>

Configuring Email Server Settings

Use the Email option to configure a security device to send messages using email whenever a system event of Emergency, Alert, Critical, or Notification severity level occurs. You can configure the email and SMTP settings at the device level, or skip this section and configure the GUI server to handle emails; see “Exporting to Email” on page 641.

To configure email server settings and enable the device to send email messages, open a device configuration and select Report Settings > Email. Configure the following settings:

Table 76: Email Server Settings for Log Entries

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Notification for Alarms</td>
<td>When alarm is enabled for a rule in the installed Security Policy and traffic matches the rule, the device sends an email notification to the specified SMTP server.</td>
</tr>
<tr>
<td>Include Traffic Log</td>
<td>When logging is enabled for a rule in the installed Security Policy and traffic matches the rule, the device sends the traffic log entry to the specified SMTP server.</td>
</tr>
<tr>
<td>SMTP Server Name</td>
<td>The name of the Simple Mail Transfer Protocol server that receives email notification messages. You must specify the SMTP server name and at least one email address to receive email notification.</td>
</tr>
<tr>
<td>Email Address 1</td>
<td>The primary email address that receives email notification messages from the device.</td>
</tr>
<tr>
<td>Email Address 2</td>
<td>The secondary email address that also receives email notification from the device.</td>
</tr>
</tbody>
</table>

Configuring Events Reporting Settings

Use the Events reporting settings to configure the security device to report specific events to NetScreen-Security Manager.
Select the appropriate NetScreen-Security Manager Device Server, then select the events that are logged on the security device and reported to NetScreen-Security Manager. The following sections detail each event.

NOTE: For security devices running ScreenOS 4.0.x, you must also select Enable Logging.

Screen Alarm Log Entries
The device generates screen alarm log entries when a security device detects network traffic that matches the screen settings enabled on the device.

To receive screen alarm log entries, you must:

- Enable the device to generate screen alarm log entries for NetScreen-Security Manager in Report Settings > NSM.
- Enable the device to send log entries with the desired severity settings to NetScreen-Security Manager in Report Settings > General > NSM.

Screen alarm log entries appear in the Log Viewer and display the following columns of information in the Log Viewer:

- Source Address
- Destination Address
- Service
- Action
- Category (Screen)
- Subcategory (for details on Screen subcategories, see “Screen Alarm Log Entries” on page 706)
- Severity

Event Alarm Log Entries
The device generates event alarms for any security event that has a predefined severity level of emergency, critical, or alert. Event alarms generate log entries that appear in the Alarm category.

To receive event alarm log entries, you must:

- Enable the device to generate event alarm log entries for NetScreen-Security Manager in Report Settings > NSM.
- Enable the device to send log entries with emergency, alert, and critical severity settings to NetScreen-Security Manager.

Event alarms appear in the Log Viewer under the Alarm category. For details on Attack subcategories, see “Alarm Log Entries” on page 707.
Traffic Alarm Log Entries
The device generates traffic alarm log entries when your security device detects network traffic that exceeds the specified alarm threshold in a Security Policy rule. The traffic alarm log entry, which displays in the Log Viewer, describes the security event that triggered the alarm. Traffic alarms generate log entries that appear in the Alarm category.

To receive traffic alarm log entries, you must:

- Enable the device to generate traffic alarm log entries for NetScreen-Security Manager in Report Settings > NSM.
- Enable the device to send log entries with the desired severity settings to NetScreen-Security Manager.
- Enable counting and alarms in the Security Policy installed on the device. For details on configuring traffic alarm logging in your Security Policy rules, see “Configuring Counting and Alarms” on page 339.

Traffic alarms appear in the Log Viewer under the Alarm category. For details on alarm subcategories, see “Alarm Log Entries” on page 707.

Alarm log entries contain information in the following Log Viewer columns:

- To Zone
- From Zone
- Source IP
- Destination IP
- Threshold (displayed in the Misc. column of the Log Viewer)

Deep Inspection Alarm Log Entries
The device generates Deep Inspection alarm log entries when a security device with Deep Inspection (DI) detects network traffic that matches an attack object specified in a Security Policy rule. When matched in a rule, protocol anomaly attack objects, signature attack objects, and custom attack objects all generate Deep Inspection alarm log entries that appear in the Log Viewer.

To receive Deep Inspection alarm log entries, you must:

- Enable the device to generate Deep Inspection alarm log entries for NetScreen-Security Manager in Report Settings > NSM.
- Enable the device to send log entries with the desired severity settings to NetScreen-Security Manager in Report Settings > General > NSM.
- Enable Deep Inspection detection in the Security Policy installed on the device. For details on configuring Deep Inspection logging in your Security Policy rules, see “Configuring a DI Profile/Enable IDP For Firewall Rules” on page 345.
Deep Inspection alarm log entries appear in the Log Viewer and display the following columns of information in the Log Viewer:

- Source Address
- Destination Address
- Service
- Action
- Category (Predefined or Custom)
- Subcategory (for details on Deep Inspection alarm subcategories, see “Deep Inspection Alarm Log Entries” on page 708)
- Severity

**Configuration Log Entries**

The device generates configuration log entries for events that change the configuration on the device. Specifically, any command issued that the ScreenOS `get config` command statement captures and displays in ScreenOS generates a configuration log. For each configuration change, the device generates a configuration log entry that contains information about the change in the Log Viewer Detail column.

To receive configuration log entries, you must:

- Enable the device to generate configuration log entries for NetScreen-Security Manager in Report Settings > NSM.
- Enable the device to send log entries with a notification severity setting to NetScreen-Security Manager in Report Settings > General > NSM.

Configuration log entries appear in the Log Viewer under the category Configuration. For details on configuration subcategories, see “Configuration Log Entries” on page 773.

**Information Log Entries**

The device generates information logs when it detects that an administrator has made a change to the basic settings of the device, such as logging in/log out, setting a new password for the device, issuing a key value for the device, or entering an MD5 authentication password to enter a device. For each administrative change, the device generates an information log entry that contains information about the change in the Log Viewer Detail column.

To receive information log entries, you must:

- Enable the device to generate information log entries for NetScreen-Security Manager in Report Settings > NSM.
- Enable the device to send log entries with the info, warning, and error severity settings to NetScreen-Security Manager in Report Settings > General > NSM.
Information log entries appear in the Log Viewer under the category Information. For details on information subcategories, see “Information Log Entries” on page 775.

**Self Log Entries**

The device generates self log entries for any packet that terminates at the device. Self log entries display information on traffic that was dropped by the security device or on traffic that terminates on the device.

To receive self log entries, you must:

- Enable the device to generate self log entries for NetScreen-Security Manager in Report Settings > NSM.
- Enable the device to send specific self log entries to NetScreen-Security Manager in Report Settings > General > Firewall Options. For details, see “Forwarding Self Log Entries (Firewall Options)” on page 592.

Self log entries appear in the Log Viewer under the category Self, which contains information in the following Log Viewer columns:

- Source
- Destination
- Services

Self log entries have the category “Self” and the subcategory “Self Log”.

**Traffic Log Entries**

The device generates traffic log entries when your security device detects network traffic that matches the source, destination, and service specified in a Security Policy rule.

To receive traffic log entries, you must:

- Enable the device to generate traffic log entries for NetScreen-Security Manager in Report Settings > NSM.
- Enable the device to send log entries with the desired severity settings to NetScreen-Security Manager.
- Enable logging in the Security Policy installed on the device. For details on configuring traffic logging in your Security Policy rules, see “Configuring Logging and Alerts” on page 338.

Traffic log entries appear in the Log Viewer under the Traffic category. For details on traffic subcategories, see “Traffic Log Entries” on page 776.
Policy Statistics
The device forwards statistics on the policy distribution of the traffic that entered the device. Policy distribution statistics do not generate log entries; the information is used by the Realtime Monitor module. For details on how policy distribution appears in Realtime Monitor, see “Viewing Traffic Distribution by Security Policy” on page 524.

Attack Statistics
The device forwards statistics for attacks detected in the traffic that entered the device. Attack statistics do not generate log entries; the statistics are used by the Realtime Monitor module. For details on how attack statistics appear in Realtime Monitor, see “Viewing Attack Statistics” on page 533.

Ethernet Statistics
The device forwards statistics for ethernet activity on the device. Ethernet statistics do not generate log entries; the statistics are used by the Realtime Monitor module. For details on how ethernet statistics appear in Realtime Monitor, see “Viewing Ethernet Statistics” on page 531.

Flow Statistics
The device forwards statistics for flows that entered the device. Flow statistics do not generate log entries; the statistics are used by the Realtime Monitor module. For details on how flow statistics appear in Realtime Monitor, see “Viewing Flow Statistics” on page 533.

Protocol Distribution
The device forwards information on the protocol distribution of the traffic that entered the device. Protocol distribution information does not generate log entries; the information is used by the Realtime Monitor module. For details on how protocol distribution appears in Realtime Monitor, see “Viewing Traffic Distribution by Protocol” on page 527.

The device reports statistics generated by the following services:

- AH (Authentication Header)
- ESP (Encapsulating Security Payload)
- GRE (Generic Routing Encapsulation)
- ICMP (Internet Control Message Protocol)
- OSPF (Open Shortest Path First)
- TCP (Transmission Control Protocol)
- UDP (User Datagram Protocol)

You can also set the interval at which the NetScreen-Security Manager Device Server polls for policy statistics and protocol distribution events.
Atomic Updating Events

Devices running ScreenOS 5.1 or higher support atomic updating, which enables the device to receive the entire modeled configuration (all commands) before executing those commands (instead of executing commands as they are received from the management system). Atomic updating also enables the device to temporarily lose connection to NetScreen-Security Manager during the update process.

If the device cannot reconnect to the management system after processing the update, it automatically reboots (with the previously saved configuration) and reconnects to the management system. To prevent a device from rebooting and/or configure the reboot timeout, open a device configuration and select Report Settings > Events, then configure the Atomic Updating options.

For details on Atomic Updating, see “About Atomic Updating (ScreenOS 5.1 or Higher Only)” on page 174.

Configuring SNMP Reporting Settings

Use SNMP settings to configure the Simple Network Management Protocol (SNMP) agent for the security device. The SNMP agent provides a view of statistical data about the network and the devices on it, and notification of system events of interest. You can configure the SNMP settings at the device level, or skip this section and configure the GUI server to handle SNMP reporting; see “Exporting to SNMP” on page 640.

In addition to configuring the SNMP reporting settings, you also must enable SNMP management service options on the interface through which the SNMP manager application communicates with the SNMP agent in the security device.

To configure SNMP settings and enable the device to send SNMP traps, open a device configuration and select Report Settings > SNMP. Configure the following settings:

- System Name—The name of the device for which you are generating SNMP status.
- Contact Person—The name of the network administrator who manages the device. This contact information is useful when the SNMP community member needs to contact someone about the device.
- Location—The physical location of the device.
- Listen Port—The number of the port assigned to monitor SNMP traffic (listen and transmit SNMP traps).
- Trap Port—The number of the port assigned to transmit traps that have been generated by an SNMP alarm, threshold violation, or error.
- Enable Authentication Fail Trap—Specifies whether you want to generate a trap if a packet fails to be authenticated when attempting to enter the device. Select this options if the device sends SNMP messages through a VPN tunnel.
Next, configure SNMP communities. To send traps, the SNMP agent on the security device requires that you define communities, their associated hosts, and assign permissions (read/write or read-only). You can create up to three (3) SNMP communities, with up to eight (8) hosts in each community.

To create an SNMP community, click the Add icon under Community Settings and configure the following settings:

- **Community name**—The device uses the community name to authorize users attempting to enter the device.
- **Access Mode**—Defines read-write or read-only privileges for the community.
- **Trap Mode**—When enabled (On), enables the device to send an SNMP trap for illegal SNMP connections attempts to the device.
- **Traffic**—When enabled, the device can accept traffic from the source interface.
- **Version**—Defines the versions supported by the community (SNMPv1, SNMPv2c, or both SNMP versions, as required by the SNMP management stations). For backward compatibility with earlier ScreenOS releases that only support SNMPv1, security devices support SNMPv1 by default.
- **Hosts**—Define the host(s) associated with the community. Click the Add icon, then specify the host IP address and netmask, the trap version for the host (if an SNMP community supports both SNMPv1 and SNMPv2c, you must specify a trap version for each community member), and the source interface.

**Directing Logs to a Syslog Server**

A security device can generate syslog messages for system events at predefined severity levels and optionally for traffic that policies permit across a firewall. It sends these messages via UDP (port 514) to up to four designated syslog hosts running on UNIX/Linux systems. When you enable syslog reporting, you also specify which interface the security devices is to use to send syslog packets.

You can configure the syslog server settings at the device level, or skip this section and configure the GUI server to handle syslog messages; see “Exporting to Syslog” on page 640.

To send log entries to a Syslog server, click the Syslog option. NetScreen-Security Manager displays the Syslog dialog box. Enter appropriate data into the following fields.

**Table 77: Syslog Settings for Log Entries**

<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>
</tbody>
</table>
Chapter 14: Logging

Using the Log Viewer

The Log Viewer displays log entries generated by a security device when traffic matches a firewall or VPN rule, or when an event occurs that matches a predefined set of conditions. The main display of the Log Viewer displays summarized information about security events and alarms, while the detail panes provide more detailed information about a specific log entry.

This section provides details on the following Log Viewer functionality:

- **Using Log Views**—The Log Viewer includes several predefined views for critical severity attacks, configuration log entries, scans, and other important activity. This section describes how to use filters to create your own unique, customized log entry view, then save the custom view (with all its filters) for future use.

### Table 78: WebTrends Settings for Log Entries

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable WebTrends Message</td>
<td>Directs NetScreen-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 the desired severity checkbox.
- **Searching Log Entries**—For networks that generate large numbers of log entries, it can be difficult to locate the exact log entries that detail the events you want to investigate. This section describes how to use the log timeline to find logs generated around a specific time, how to use the find utility to locate log entries with a specific value, and how to search by LogID to jump directly to a specific log entry.

- **Filtering Log Entries by Event and Time**—This section describes how to create custom filters based on event data or time. You can apply these filters to a Log Viewer column or cell to reduce the number of log entries that appear in the main display area, helping you to focus your investigations on a specific group of log entries.

- **Filtering Log Entries by Range**—This section describes how to create custom filters based on a user-defined range. You can apply these filters to a Log Viewer column or cell to reduce the number of log entries that appear in the main display area, helping you to focus your investigations on a specific group of log entries.

- **Customizing Columns**—The Log Viewer includes 40 columns of log entry information; however, each predefined view includes only a small subset (16) of available columns. This section describes how to set viewable columns, change column display order, resize columns, and hide/unhide a specific column.

- **Using Log Viewer Integration**—This section describes how to use the Log Viewer integration to jump from a log entry directly to the responsible Security Policy or managed device configuration.

- **Identifying Irrelevant Attacks**—Irrelevant attacks are events that do not affect your network or that you do not consider important. For example, if you do not run an Apache Web server on your network, you do not need to worry about attacks against Apache Web servers. This section describes how to use your log entries to identify irrelevant attacks, then eliminate the attack object group that generated that attack from your Security Policy.

### Using Log Views

The Log Viewer enables you to view and analyze logs generated by the managed devices in your network. For your convenience, several predefined views are included for critical severity attacks, configuration log entries, scans, and other important activities. Using filters, you can create your own unique, customized log entry view, then save the custom view (with all its filters) and manage them in folders for future use.

**About Predefined Log Views**

Table 79 lists and describes these predefined log views.
Table 79: Log Categories

<table>
<thead>
<tr>
<th>Log Type</th>
<th>Displays all logs filtered by</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>Severity level - Critical</td>
</tr>
<tr>
<td>Alarm</td>
<td>Category - Alarm</td>
</tr>
<tr>
<td>IDP/DI</td>
<td>Category - Custom, Predefined</td>
</tr>
<tr>
<td>Screen</td>
<td>Category - Screen</td>
</tr>
<tr>
<td>Traffic</td>
<td>Category - Traffic</td>
</tr>
<tr>
<td>Info</td>
<td>Category - Info</td>
</tr>
<tr>
<td>Config</td>
<td>Category - Config</td>
</tr>
<tr>
<td>Self</td>
<td>Category - Self</td>
</tr>
<tr>
<td>Custom</td>
<td>Category - Custom</td>
</tr>
<tr>
<td>Backdoor</td>
<td>Subcategory - Backdoor Detected (Traffic), Backdoor Dropped (Traffic)</td>
</tr>
<tr>
<td>PolicyLogViewer</td>
<td>Policy, Rule #, Rule Domain, Rule Domain Version, Rulebase</td>
</tr>
<tr>
<td>Profiler</td>
<td>Category - Profiler</td>
</tr>
<tr>
<td>Scans</td>
<td>Subcategory - Distributed Port Scan, Distributed Port Scan In Progress, ICMP Sweep, ICMP Sweep In Progress, Network Scan, Network Scan In Progress, TCP Port Scan, TCP Port Scan In Progress, TSIG Session Rate Exceeded, UDP Port Scan, UDP Port Scan In Progress</td>
</tr>
</tbody>
</table>

Creating Custom Views and Folders

A custom view enables you to organize log entries in a format that is most helpful to you. Because the custom view is based on filters, incoming log entries that match the filter criteria are automatically displayed in the view (you do not need to re-apply the view to new logs).

You might want to create views to help manage the following situations:

- **Workflow**—To help a team of security administrators work together to investigate and resolve incidents, create a view that filters on the flag column of the Log Viewer to indicate the status of each log entry and assignment.

- **Attackers**—To track the activities of a known attacker, create a view that filters on a specific source IP. The source IP address of an attack displays in the source address column, and the destination IP address of an attack displays in the destination address column.

- **Alarms**—To quickly access log entries generated by a policy rule that contains an alarm, create a view that filters on the alarm column. This method is useful when you are fine-tuning policies to distinguish between genuine attacks and false positives.

- **Devices**—To manage devices in multiple locations that use different investigation processes, create a separate view for each device at a specific location.

You can create and save custom views using one of the following methods:
Create New View—First in the navigation tree, select the Log Viewer module. From the file menu, select **File > New View**. In the new view dialog box, enter a name for the custom view, enter a name for the folder that you want to save the view in, and click OK; the new view appears in the navigation tree in the folder specified. By default, all new views are saved in the Others folder. In the main display area, you can then set the desired filters for the log entries.

Set Filters—in the Log Viewer main display area, set the desired filters for the view. From the file menu, select **File > Save As**. In the new view dialog box, enter a name for the custom view, enter a name for the folder that you want to save the view in, and click OK; the new view appears in the navigation tree in the folder specified.

Creating Per Session Views
Log views that you create on the fly also called “transient” views (i.e., views set from filters defined in the Report Manager), appear in the Drill Down folder. These views remain in this folder until you logout of the UI.

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 Zone</td>
<td></td>
<td>Source zone associated with a traffic log entry. Note: Log entry data for this column only appears after you update the security device. The source zone is the zone that is attempting to send the traffic through the security device.</td>
</tr>
<tr>
<td>Source Address</td>
<td>--</td>
<td>Indicates the address of the source device that generated the packet that generated the log.</td>
</tr>
<tr>
<td>Src Port</td>
<td>Default</td>
<td>Indicates the TCP/UDP port number of the source device that generated the packet that generated the log.</td>
</tr>
<tr>
<td>Destination Address</td>
<td></td>
<td>Destination zone associated with a traffic log entry. Log entry data for this column only appears after you update the security device.</td>
</tr>
<tr>
<td>Dst Port</td>
<td>Default</td>
<td>Indicates the destination device to which the packet associated with the log entry was targeted.</td>
</tr>
<tr>
<td>Column</td>
<td>Default</td>
<td>What it means</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Protocol</td>
<td>Default</td>
<td>The connection type or protocol of the matching traffic. Protocols also have one or more port numbers.</td>
</tr>
<tr>
<td>Device Address</td>
<td>--</td>
<td>Indicates the address of the server.</td>
</tr>
<tr>
<td>Comment</td>
<td>Default</td>
<td>Enables you to add a comment that relates to the generated log entry. To enter a comment, click in the cell and enter text.</td>
</tr>
<tr>
<td>Category</td>
<td>Default</td>
<td>Indicates what type of log you are viewing. Can be expressed either as a category or a sub-category. A category is either an alarm, config, misc, or traffic. A sub-category is an attack type.</td>
</tr>
<tr>
<td>Sub Category</td>
<td>Default</td>
<td>Indicates the subcategory of the log you are viewing.</td>
</tr>
<tr>
<td>Packet Data</td>
<td>--</td>
<td>Indicates the traffic type designated as part of the log entry. This indication is used to identify a packet entry created in the rulebase.</td>
</tr>
<tr>
<td>Severity</td>
<td>Default</td>
<td>Indicates the level of severity associated with the attack detected. Every attack has a default severity level although you can configure a different one.</td>
</tr>
<tr>
<td>Log ID</td>
<td>--</td>
<td>Indicates the unique identifier ID for the log entry. The log ID comprises both a date and an incrementing integer.</td>
</tr>
<tr>
<td>Action</td>
<td>--</td>
<td>Indicates whether an action occurred in response to the event that generated the log.</td>
</tr>
<tr>
<td>Alert</td>
<td>--</td>
<td>Indicates whether an alert flag was generated in response to the event that generated the log.</td>
</tr>
<tr>
<td>Application Name</td>
<td>--</td>
<td>Indicates the application associated with the current log.</td>
</tr>
<tr>
<td>Bytes In</td>
<td>--</td>
<td>Indicates the number of bytes that comprised the log data entering the Log Viewer.</td>
</tr>
<tr>
<td>Bytes Out</td>
<td>--</td>
<td>Indicates the number of bytes that comprised the log data being transmitted from the Log Viewer.</td>
</tr>
<tr>
<td>Bytes Total</td>
<td>--</td>
<td>The sum of the number of bytes transmitted and received by the Log Viewer.</td>
</tr>
<tr>
<td>Device</td>
<td>--</td>
<td>Indicates the IP address of the device that generated the current log.</td>
</tr>
<tr>
<td>Device Domain</td>
<td>--</td>
<td>Indicates the name of the domain in which the device resides. Note: The Log Viewer displays log entries for a single domain at a time. By default, when logged in as the super admin, the Log Viewer displays log entries for managed devices in the global domain. To change the domain, apply a domain filter to view log entries for managed devices in a specific domain.</td>
</tr>
<tr>
<td>Domain Ver</td>
<td>--</td>
<td>Indicates the version number of the device.</td>
</tr>
<tr>
<td>Elapsed Secs</td>
<td>--</td>
<td>The number of seconds that have elapsed since the beginning of the current session.</td>
</tr>
<tr>
<td>From External</td>
<td>--</td>
<td>Specifies if the packet that generated this log came from an untrusted network.</td>
</tr>
<tr>
<td>Has Log Action</td>
<td>--</td>
<td>Indicates the action the device performed on the packet or connection that generated the log, generally either a permit or denial of the packet into the device.</td>
</tr>
<tr>
<td>Has Packet Data</td>
<td>--</td>
<td>Specifies if this log has associated packet data.</td>
</tr>
</tbody>
</table>
After importing a device configuration, log entries from that device begin to appear in the Log Viewer. Note however, that the following log fields for devices running a specific version of ScreenOS display 0 (or unknown) until you update the device from NetScreen-Security Manager:

- For devices running ScreenOS 5.x: domain, domain version, rulebase, policy, rule number.

<table>
<thead>
<tr>
<th>Column</th>
<th>Default</th>
<th>What it means</th>
</tr>
</thead>
<tbody>
<tr>
<td>In Eth</td>
<td>--</td>
<td>The name of the Ethernet interface that receives packets transmitted from an external device.</td>
</tr>
<tr>
<td>Misc</td>
<td>--</td>
<td>A miscellaneous string associated with the current log.</td>
</tr>
<tr>
<td>NAT Dst Port</td>
<td>--</td>
<td>A destination port associated with the packet that has generated the log that has also undergone a network address translation.</td>
</tr>
<tr>
<td>NAT Src Port</td>
<td>--</td>
<td>A source port associated with the packet that has generated the log that has also undergone a network address translation.</td>
</tr>
<tr>
<td>NAT Dst Addr</td>
<td>--</td>
<td>A destination address associated with the packet that generated the log that also undergone a network address translation.</td>
</tr>
<tr>
<td>NAT Src Addr</td>
<td>--</td>
<td>The source address associated with the packet that generated the log that has also undergone a network address translation.</td>
</tr>
<tr>
<td>Out Eth</td>
<td>--</td>
<td>The name of the Ethernet interface that transmits packets to an external device.</td>
</tr>
<tr>
<td>Packets In</td>
<td>--</td>
<td>Specifies the number of received packets for a given session on the current port.</td>
</tr>
<tr>
<td>Packets Out</td>
<td>--</td>
<td>Specifies the number of transmitted packets for a given session on the current port.</td>
</tr>
<tr>
<td>Packets Total</td>
<td>--</td>
<td>Specifies the aggregate number of both received and transmitted packets for a given session on the current port.</td>
</tr>
<tr>
<td>Policy</td>
<td>--</td>
<td>The name of the policy that generated the log.</td>
</tr>
<tr>
<td>Role</td>
<td>--</td>
<td>Role associated with a specific application.</td>
</tr>
<tr>
<td>Rule #</td>
<td>--</td>
<td>The rule in the rulebase in the policy in the specific version of a domain that generated this log.</td>
</tr>
<tr>
<td>Rule Domain</td>
<td>--</td>
<td>The domain that contained the rule that generated this log.</td>
</tr>
<tr>
<td>Rulebase</td>
<td>--</td>
<td>The rulebase inside the policy in a specific version of a domain that generated this log.</td>
</tr>
<tr>
<td>Time Generated</td>
<td>--</td>
<td>The time the current log was generated.</td>
</tr>
<tr>
<td>URI</td>
<td>--</td>
<td>Indicates the Universal Resource Indicator (URI) associated with the current log.</td>
</tr>
<tr>
<td>User Flag</td>
<td>--</td>
<td>The GUI assignable flag associated with the current log.</td>
</tr>
<tr>
<td>Vsys</td>
<td>--</td>
<td>The name of the virtual system that generated the current log.</td>
</tr>
<tr>
<td>Var Data</td>
<td>--</td>
<td>Indicates the kind of variable data if any associated with the current log.</td>
</tr>
<tr>
<td>Log ID</td>
<td>--</td>
<td>A value that represents the sequential record ID of the log for the specified day. In the format the nth log received.</td>
</tr>
</tbody>
</table>
For devices running ScreenOS 4.0.x: domain, domain version, rulebase, policy, rule number, from zone, to zone, action.

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

Log Viewer Detail Panes
The Log Viewer contains additional panes that provide summary and detail information for log entry events. To see detailed information about a log entry, select the entry and view the detail panes at the bottom of the Log Viewer. The detail pane contains three tabs of information about the selected log record:

- Summary tab (default tab)—Details the event associated with the selected log entry. Within the summary tab, you can view the event description (right side) and the variable data (left side). Not all log entries contain variable data—only log entries generated by an attack provide variable data.

- All Fields tab—Provides a condensed view of data for the selected log entry (so you don’t need to scroll from horizontally).

- Whois tab—Enables you to perform a Whois lookup on an IP address to see what organization has registered a particular address.

- Quick Reports—Enables you to quickly generate a predefined report on a filter criteria in the Log Viewer.

Log Viewer Status Bar
The status bar of the Log Viewer summarizes the filters applied to log entries in the log entry list. In the status bar, the filter type description appears; to view filter details, place the cursor over the filter type.

For example, the status bar below displays the filter types Category and Severity:

Figure 185: View Category and Severity Filters Messages

Navigating the Log Viewer
Using the side scroll bar, you can navigate through hundreds of log entries quickly and precisely:
Log entries higher in the list are older than log entries at the bottom of the list. To navigate through log entries based on a specific time, use the Log Timeline (for details, see “Log Timeline” on page 609).

Searching Log Entries

The Log Viewer can receive thousands or even millions of log entries each day. To quickly locate a specific log entry or logs, use the following log searching tools:

Table 81: Search Tools for Log Viewer

<table>
<thead>
<tr>
<th>Tool</th>
<th>Description</th>
<th>Benefit</th>
</tr>
</thead>
</table>
| Log Timeline     | A 14-day timeline that enables you to zoom to log entries for a specific day and time. | Specify an exact date and time, or use the timeline selection slider to move immediately to a specific day’s log entries.  
|                  |                                                                             | Can also use the Tailing Logs feature to jump directly to incoming log entries.            |
|                  |                                                                             | Timeline covers any 14-day period, in increments of days, hours, or minutes.               |
| Flags            | A symbol used to tag a specific log entry that you want to return to at a later point. The flagged entry stands out from other entries, making it easier to locate quickly. | Gain greater control over identifying events.  
|                  |                                                                             | Flags are colorful and iconic, making them more visible than text-based results of filters.|
|                  |                                                                             | You can filter on a flag setting.                                                         |
| Find Utility     | A string search that searches for a log entry based on a character string in the reported event. | Locate a specific event quickly with minimal detail; for example, search using the timestamp or IP address field.  
|                  |                                                                             | Move quickly from one relevant event to another, avoiding scrolling.                      |
| Log ID Number    | A value search that searches for a log entry based on the log ID number.      | Locate a specific log entry immediately.  
|                  |                                                                             | Typically, you use a log ID search when you have previously viewed the log entry and need to find it again quickly. |
The following sections detail each search tool.

**Log Timeline**

The log timeline is a powerful tool that enables you quickly jump to a group of log entries generated during a specific time period.

The timeline consists of 4 components: the time slider, time entry, time blocks, and Tailing Logs. The following sections detail each component.

**Using the Time Slider**

The time slider marks the midpoint of the time interval selected for the timeline (for details on setting a time interval, see “Using Time Blocks” on page 610). You can move the time slider to the desired time using your mouse cursor: Click the slider, then drag it to the area on the timeline that represents the time around which you want to view log entries, as shown below:

![Log Viewer Time Slider](image)

**Using Time Entry**

You can also enter a date and time into the log timeline directly. Select the time display, then enter the desired time and click Go.

![Log Viewer Time Display](image)
Using Time Blocks
To change the log timeline intervals, select a specific time block or use the Out and In buttons. From left to right, the time blocks are:

- 14 days
- 7 days
- 3 days
- 1 day
- 12 hours
- 6 hours
- 3 hours
- 1 hour
- 30 minutes
- 1 minute

Clicking the Out button selects the time block to the left of the currently selected time block; clicking the In button selects the time block to the right of the currently selected time block. Alternatively, you can use the mouse wheel on your mouse to adjust the time interval.

Using Tailing Logs
To view arriving log entries, select Tailing Logs. The log entry list automatically jumps to the bottom of the list, where new log entries display when they are received by the management system. As older log entries are moved up by arriving log entries, the view remains fixed at the bottom of the list.

Tailing Logs also works with filters, predefined view, and custom views.

EXAMPLE: TAILING INCOMING LOGS IN THE LOG VIEWER
To see configuration log entries as they arrive from a specific device:

1. Select the 7-Config view from the Log Viewer navigation tree. This view uses a predefined filter to display log entries with the category “configuration” only.

2. Set a custom filter to set log entries from a specific device (for details, see “Filtering Log Entries by Event and Time” on page 612). The view changes to display configuration log entries from that device.

3. Select Tailing Logs. The view jumps to the bottom of the log entry list, and remains there; as new configuration log entries for the device arrive, they appear at the bottom of the list.
Using Flags

Use a flag to mark a specific event with a severity or workflow marker. Applying a flag to a log entries helps the event stand out from other log entries. The following table displays a list of log filter symbols.

Table 82: Log Viewer Flags

<table>
<thead>
<tr>
<th>Filter Symbol</th>
<th>Severity Level</th>
<th>Filter Type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Low</td>
<td>Severity</td>
</tr>
<tr>
<td></td>
<td>Medium</td>
<td>Severity</td>
</tr>
<tr>
<td></td>
<td>High</td>
<td>Severity</td>
</tr>
<tr>
<td></td>
<td>Assigned</td>
<td>Information</td>
</tr>
<tr>
<td></td>
<td>False Positive</td>
<td>Information</td>
</tr>
<tr>
<td></td>
<td>Closed</td>
<td>Information</td>
</tr>
<tr>
<td></td>
<td>Follow-Up</td>
<td>Information</td>
</tr>
<tr>
<td></td>
<td>Pending</td>
<td>Information</td>
</tr>
</tbody>
</table>

Within the Log Viewer, you can set a filter on one or more flags. Additionally, within Report Manager, you can generate a report that displays the count of all log entries that contain a specific flag.

Using the Find Utility

Use the Find utility to search for the next iteration (down) of a value in the Log Viewer. To use Find on a column or cell, right-click the column header or cell and select Find, then configure the search criteria. Select Negate to search for all log entries that do not contain the specified value.
Using Log ID Number

When you know the Log ID number for the log entry, you can jump directly to the log entry. To locate a log entry by Log ID number, from the file menu, select Edit > Go To Log ID. In the Go To Log ID dialog box, enter the log ID number click OK. The Log Viewer jumps to the specified Log ID and highlights the log entry in the main display area.

Filtering Log Entries by Event and Time

An event- or time-based filter is a criteria search for matching log entries. When you apply a filter to log entries, the Log Viewer filters out log entries that do not match the filter criteria. You can set multiple filters on any Log Viewer column (except Log ID and Details) or cell value.

When filtering by cell, the filter affects only the content in that cell’s column. To set a cell filter, right-click a cell and select Filter to display the filter menu options:

- Edit—Use this option to set multiple filters for cell content at the same time. Select to display the Filter dialog box for that column, then select the columns you want to filter on.
  - To display only the selected content, click OK.
  - To display everything except the selected content, click the checkbox next to Negate, then click OK.
  - To clear filters for the selected content, click Clear.

- Only This Value—Displays only the content in the selected cell.

- Not This Value—Displays everything except the content in the selected cell.

- Clear Filter—Removes a current filter on the selected cell content. If no filter exists, this option is unavailable.

- Clear All Filters—Removes all filters on the current view.

When filtering by column, the filter affects all log entries. You can set an event-based filter using any log entry column that contains event data, and a time-based filter for the Time Generated and Time Received columns. Additionally, for all filters (cell or column), you can enable the Negate option to match all log entries that do not contain the specified filter criteria.

NOTE: You cannot apply a filter to the Log ID or Details column.

The following sections detail some common event- and time-based filters used to manage log entries.

Setting a Category Filter

Apply a category filter to view log entries within a specific category or subcategory.
To create a category filter, right-click the Category column header and select Filter > Set Filter. Select the categories you want to use as the filter criteria, then click OK. NetScreen-Security Manager applies the filter to all log entries and displays only the log entries that match the specified category.

To create a subcategory filter, right-click the Subcategory column header and select Filter > Set Filter. Select the category first, then select the subcategories you want to use as the filter criteria, then click OK. NetScreen-Security Manager applies the filter to all log entries and displays only the log entries that match the specified subcategory.

Setting an Alert Filter
Apply an alert filter to view log entries that have an enabled or a disabled alert state. To create an alert filter, right-click the Alert column header and select Filter > Set Filter, then configure the alert filter settings:

- To display log entries that contain an enabled alert, select On and click Ok.
- To display log entries that contain a disabled alert, select Off and click Ok.

NetScreen-Security Manager applies the filter to all log entries and displays only the log entries that match the specified alert state.

Setting a Flag Filter
Apply a flag filter to view log entries that have a specified flag type. To create a flag filter, right-click the Flag column header and select Filter > Set Filter. Select the flag types that you want to use as the filter criteria, then click OK. NetScreen-Security Manager applies the filter to all log entries and displays only the log entries that match the specified flag type.

**NOTE:** The Unflagged option in the flag filter can be helpful when trying to locate log entries that do not have assigned flags. When setting the flag criteria, select Unflagged as the flag type; NetScreen-Security Manager then displays all log entries without flags.

Setting an Address Filter
Apply an address filter to view log entries that record events for a specific source or destination address, or source or destination NAT address. To create an address filter, right-click the Src Addr, Dst Addr, NAT Src Addr, or NAT Dst Addr column header and select Filter > Set Filter. Select “Click here to add address” and enter a valid IP address and click Ok. For NAT addresses, enter the IP address that is translated and click Ok.

NetScreen-Security Manager applies the filter to all log entries and displays only the log entries that match the specified IP address.
Setting a Protocol Filter

Apply a protocol filter to view log entries for events that use a specific protocol type. To create a protocol filter, right-click the Protocol column header and select Filter > Set Filter. Select the protocol types that you want to use as the filter criteria, then click OK. NetScreen-Security Manager applies the filter to all log entries and displays only the log entries that match the specified protocol types.

Setting a Domain Filter

The Log Viewer display log entries for a single domain at a time. By default, when logged in as the super admin, the Log Viewer displays log entries for managed devices in the global domain. To change the domain, apply a domain filter to view log entries for managed devices in a specific domain.

To create a domain filter, right-click the Domain column and select Filter > Set Filter. Select the domain for which you want to view log entries, then click OK. NetScreen-Security Manager applies the filter to all log entries and displays only the log entries that are generated from managed devices in the specified domain.

Setting a Time-Based Filter

Apply a time-based filter to view log entries generated or received within a specific time period. To create a time-based filter, right-click the Time Generated or Time Received column and select Filter > Set Filter:

- To filter on a specific start time, select From and configure the start date and time. When applied, this filter displays log entries for events that were generated or received after or at the specified start time.

- To filter on a specific end time, select To and configure the end date and time. When applied, this filter displays log entries for events that were generated or received before or at the specified end time.

- To filter on a time period, select From and To, then enter the start and end date and time. When applied, this filter displays log entries for events that were generated or received within the specified time period.

EXAMPLE: USING FILTERS IN THE LOG VIEWER

In this example, you want to view all critical and major severity log entries that have a Follow-Up flag assigned to them. Additionally, you want to limit the search to log entries generated by the Engineering NSRP cluster on your network.

1. In the Log Viewer, right click the severity column header and select Filter > Set Filter. Enable Major and Critical, then click to save and apply the filter to your log entries.

2. Right click the User Flag column header and select Filter > Set Filter. Enable Follow-Up, then click OK to save and apply the filter to your log entries.

3. Right click the Device column header and select Filter > Set Filter. Select Engineering Cluster, then click OK to save and apply the filter to your log entries.
Filtering Log Entries by Range

A range filter is a criteria search for matching log entries within a value range. You can set a range filter for the following columns:

- Bytes In/Bytes Out
- Bytes Total
- Packets In/Packets Out
- Packets Total
- Src Port/Dst Port
- NAT Src Port/NAT Dst Port
- Elapsed Seconds

The following sections detail some common range filters used to manage log entries.

Setting a Bytes In/Out Range Filter

To view log entries based on the number of bytes received or transmitted during the event, set a range filter on the Bytes In or Bytes Out column:

1. Right-click the Bytes In or Bytes Out column header and select Filter > Set Filter. The Bytes In/Bytes Out filter dialog box appears.

2. Set the range for bytes received (Bytes In) or transmitted (Bytes Out):
   a. To filter on a minimum number of bytes only, select From and enter a value. When applied, this filter displays log entries for events that received or transmitted more than or equal to the specified minimum number of bytes.
   b. To filter on a maximum number of bytes only, select To and enter a value. When applied, this filter displays log entries for events that received or transmitted fewer than or equal to the specified maximum number of bytes.
   c. To filter on a range of bytes, select From and To, then enter the minimum and maximum values for the range. When applied, this filter displays log entries for events that received or transmitted a number of bytes within the specified range.

3. Click OK to apply the filter.

NOTE: By default, the Log Viewer does not display the Bytes In or Bytes Out column. To set a byte filter, you must first configure the Log Viewer to display these columns. For details on configuring column settings, see “Customizing Columns” on page 616.
Setting a Port Number Range Filter

To view log entries based on a range of port numbers used in the event, set a range filter on the Dst or Src Port column:

1. Right-click the Src Port or Dst Port column header and select Filter > Set Filter. The Dst/Src Port filter appears.

2. Set the range for the port numbers:
   a. To filter on a minimum port number only, select From and enter a value. When applied, this filter displays log entries for events that used a port greater than or equal to the specified minimum port number.
   b. To filter on a maximum port number only, select To and enter a value. When applied, this filter displays log entries for events that used a port less than or equal to the specified maximum port number.
   c. To filter on a range of port numbers, select From and To, then enter the minimum and maximum values for the range. When applied, this filter displays log entries for events that used ports within the specified range.

3. Click OK to apply the filter.

Customizing Columns

You can configure the Log Viewer to display specific columns.

Using Column Settings

The Log Viewer includes 40 columns of log entry information; however, each predefined view includes only a small subset (16) of available columns. To view information in the other available columns, or to change the column display order, you can adjust the column settings for the view.

The more columns you configure to appear in the Log Viewer, the more information you can see at one time—and the more you must scroll from side to side to view all columns; setting fewer columns means less viewable information, but also less scrolling. Typically, you use fewer columns when you already have enough detail about the event and/or you are only interested in specific event data.

Use column selection in combination with filters to create a customized view of your log entries.

Hide/ Unhide/ Move Columns

You hide, unhide, or move columns to display specific information using one of the following methods:

- When managing columns using the Column Settings dialog box:
  - To display hidden columns, select the columns and click Show.
  - To hide columns, select the columns and click Hide.
To reorder the column display sequence, select a column and click Move Up and Move Down.

When managing columns in the main display area:

- To hide a column, right-click the column header and select Hide Column. To unhide a hidden column, you must use the Column Settings dialog box.
- To reorder the column display sequence, select a column and drag it to the new location.
- To change column width, select the left or right edge of the column header and drag the edge to the desired width.

**EXAMPLE: CUSTOMIZING LOG VIEWER COLUMNS**

In this example, you want to view the following information in the Log Viewer:

- The attacks that attempt to enter your network.
- The source IP and port of the attacking computers.
- The destination IP and port on the target computers.
- The date and time of the attacks.
- The devices that detected the attack.
- The policies that matched the attack.

First, you configure the Log Viewer to display only the columns that contain the information you are interested in viewing, then you set can filters on those columns to narrow your search.

To configure the column settings:

1. In the navigation tree, select the Log Viewer module.
2. From the file menu, select View > Choose Columns. NetScreen-Security Manager displays the Column Settings dialog box, listing all 40 columns.
3. Select the following columns:
   - Time Received
   - Src Addr
   - Dst Addr
   - Dst Port
   - Category
   - Subcategory
   - Device
Using the Log Viewer

Ensure all other columns are not selected, then click OK to apply your changes to the Log Viewer.

4. In the main display area, select the Src Port column header, then drag and drop the column to the right of the Src Addr column.

To configure the column filters:

1. In the main display area, right-click the Category column header and select Filter > Set Filter. The Category filter dialog box appears.

2. Select the following categories: Predefined, Custom, and Screen. Click OK to apply your changes. The Log Viewer applies the filter to the log entries.

Using Log Viewer Integration

The Log Viewer module is integrated with Security Policies and Device Manager modules. This integration enables you to jump from a log entry in the Log Viewer directly to the responsible Security Policy (Jump to Rule) or managed device (Jump to Device Configuration).

Jump to Policy

To quickly edit a Security Policy rule from the Log Viewer, right-click a log entry and select Jump to Policy. NetScreen-Security Manager opens a new UI window and displays the policy with the rule that generated the log entry.

- If the responsible rule exists within a rule group, the group is automatically expanded to reveal the rule.

- If the responsible rule exists within a VPN created by VPN Manager, the autogenerated rules appear.

Depending the domain version of the Security Policy, the rule might display as read/write or read-only.

Domain version refers to a specific modeled configuration; each time you install a modeled configuration (this includes Security Policies) on a managed device using NetScreen-Security Manager, the management system creates a new domain version using the install date and time. NetScreen-Security Manager uses domain versions to detect differences between the running configuration (installed on the physical device) and modeled configuration. Domain versioning also enables you to view previous domain versions. For details on domain versions, see “Domain Versioning” on page 72.

Other options for archiving and restoring logs and configuration data are also available. For more information, refer to the NetScreen-Security Manager Installer Guide.
When using the Jump to Policy option in the Log Viewer, NetScreen-Security Manager compares the domain version of the managed device to the current domain version. If the responsible rule exists in a Security Policy that has the same domain version as the Security Policy installed on the managed device, you can edit the rule.

However, if the responsible rule exists in a Security Policy that has a different domain version from the Security Policy installed on the managed device, you cannot edit the rule. This typically occurs when you install a Security Policy on a managed device, then edit that policy in the NetScreen-Security Manager UI but do not update the device with the new policy changes. Because the responsible rule exists in a policy that belongs to a previous domain version, you cannot make changes to it.

Jump to Device Configuration

To quickly configure a parameter on an individual device from the Log Viewer, double-click a device in the Device column. NetScreen-Security Manager displays the device configuration for the device, enabling you to make changes to the device.

Identifying Irrelevant Attacks

Your log entries are a valuable tool in helping you identify irrelevant attacks. Irrelevant attacks are events that do not affect your network or that you do not consider important. Typically, you want to identify irrelevant attacks to:

- Reduce the number of log entries and increase system performance.
- Isolate log entries for harmless attacks.
- Focus on log entries for attacks to which you are actually vulnerable.

Select a log entry generated by a protocol anomaly or signature attack object, then view the Summary panel to see the attack description. An example is shown below:

Figure 189: Viewing Summary Panel

Look carefully at the information about affected systems, and compare it with what you know about your network. Use the following information to help you determine if the attack is relevant:
Using the Log Investigator

The Log Investigator module enables you to investigate patterns and trends on your network using data gathered from your log entries. Log entries are generated by a security device when traffic matches a Security Policy rule, or when an event occurs that matches a predefined set of conditions. The Log Investigator uses the event data recorded in the log entry to identify the destination IP addresses and ports that are attacked most frequently, the services that are used to attack most frequently, and the source IP addresses that most frequently generate attacks.

When using NetScreen-Security Manager to manage large networks with multiple managed devices, you can potentially receive several hundred log entries in a single day (depending on how you have configured your devices for logging). The Log Investigator is a helpful tool for manipulating and correlating a large volume of log entry data so you can identify and analyze important activity that might threaten your network. By analyzing your data and then using that knowledge to proactively fine-tune your Security Policies, you can decrease risk while increasing security.

This section provides details on the following Log Investigator functionality:

- **About the Log Investigator UI**—The Log Investigator main display area includes a filter summary, a log entry matrix, and two detail panes that display detail information in table and chart format.

- **Configuring Log Investigator Options**—Configure the criteria the Log Investigator uses to create the matrix, including the time period, Left and Top Axes settings, the data point count (the number of data points the Log Investigator must collect before displaying data), and the maximum number of log entries you want the Log Investigator to use when collecting data.

- **Setting Log Investigator Filters**—As in the Log Viewer, you can set filters on log entry data so the Log Investigator displays only the information you want to see. Apply multiple filters to data for all log entry columns found in the Log Viewer.

---

Table 83: Irrelevant Vs. Relevant Attacks

<table>
<thead>
<tr>
<th>Irrelevant Attacks</th>
<th>Relevant Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack target hardware you do not use.</td>
<td>Attack attempts to exploit vulnerabilities in the hardware you use in your network.</td>
</tr>
<tr>
<td>Example: Attacks that exploit Cisco routers do not affect Lucent routers.</td>
<td></td>
</tr>
<tr>
<td>Attack target software you do not use.</td>
<td>Attack attempts to exploit vulnerabilities in the software running on your network.</td>
</tr>
<tr>
<td>Example: Attacks that exploit Microsoft IIS Web servers do not affect Apache Web servers.</td>
<td></td>
</tr>
<tr>
<td>Attack target software versions you do not use.</td>
<td>Attack attempts to exploit vulnerabilities in the software versions running on your network.</td>
</tr>
</tbody>
</table>

If the attack is irrelevant, you can remove the matching Attack Object group from the rule that triggered the log entry, or monitor the Attack Object group using custom severity setting.
Investigating Log Entry Data—After you have configured the Log Investigator filters, time period, and data options, you are ready to begin investigating your log entry information. Within any cell the Log Investigator table, you can right-click and select an option to view specific details, including Destination Ports, Subcategories, and Time Period.

About the Log Investigator UI

The main display of the Log Investigator is shown below:

Figure 190: Log Investigator UI Overview

The Log Investigator contains the following UI components:

- **Filter Summary**—Displays the column/category filters currently applied to the Log Entry Matrix.
Selected Log Entries—Displays the number of log entries currently selected in the Log Entry Matrix.

Left Axis—The controlling axis for log entry data (the independent axis). The Log Investigator collects log entry data for the Left Axis setting, which determines data set that is used for Top Axis setting.

Top Axis—The controlled axis for log entry data (the dependent axis). The Log Investigator collects log entry data for the Left Axis setting; for the Top Axis setting, the Log investigator collects data that matches both the Left Axis and Top Axis setting.

Zoom Table—Displays a table of log entry details. You can view Source, Destination, Destination Port, Attack Subcategories, or Time Period details for any cell, row, or column.

Zoom Chart—Displays a chart of log entry details. You can view Source, Destination, Destination Port, Attack Subcategories, or Time Period details for any cell, row, or column.

Configuring Log Investigator Options

The first step in using the Log Investigator is to configure the basic criteria used to create the Log Investigator matrix. Initially, the default options are used; to edit these options, from the file menu, select View > Set Log Investigator Options. Using the Log Investigator Options dialog box, configure the desired settings (detailed below) and click OK to apply your changes.

The following sections detail each Log Investigator option.

Configuring a Time Period

The time period setting narrows the log entries included in your investigation based on a specified time interval or start time. Each log entry contains a timestamp that indicates the date and time the managed device generated the log entry (Time Generated). The Log Investigator compares the timestamp of a log entry to the specified time period setting, and eliminates those log entries that do not meet the time criteria.

First, you must specify a time duration. To specify a time interval for which you want to see log entries, set the number of weeks, days, hours, minutes, or seconds. Setting a longer interval time can you identify broad trends in your network activity. Typically, you want to use a longer interface time to initially locate problems. After you have identified the issues you want to investigate, set a shorter time interval to eliminate irrelevant log entry data.

After you have determined the time interval, you must set the end or start time for the duration:

NOTE: You can configure up to 20 Log Investigator sessions. To change this default number of sessions, edit the following parameter in the devSvr.cfg file (located in the management system directory /usr/netscreen/DevSvr/var/):

devSvr.irMaxIndexCount
To set the end time of the duration, select Most Recent (this is the default setting). The Log Investigator uses the current date and time as the end point for the time duration. For example, for a time interval of 5 hours, the Log Investigator collects data from log entries that have timestamps within the previous 5 hours.

To set the start time of the duration, select Start Time and configure the start date and time. The Log Investigator uses the specified date and time as the start point for the time duration. For example, for a time interval of 5 hours and a start date of 5/12/04 8:00:00AM, the Log Investigator collects data from log entries that have timestamps from the start date to the start date + 5 hours.

Typically, use Most Recent to investigate recurring activity or to monitor expected network changes. Use a start time when investigating past known events, such as a virus attack.

When using a large time interval, the number of matching log entries might exceed the capacity of the Log Investigator (100 log entries), causing a warning message to appear next to the Selected Logs indicator. If you do not make changes to the time interval filter, the Log Investigator automatically clears the session, requiring you to create a new time filter.

**EXAMPLE: SETTING A TIME INTERVAL IN THE LOG INVESTIGATOR**

On Friday afternoon, you want to investigate attacks received by your network in the last seven hours. Configure the time period as shown below:

![Figure 191: Configure Time Period Filter](image)

On Monday morning, you want to investigate attacks received by your network during the last work week. If Monday’s data is 5/17/04, you configure the time period as shown below:

![Figure 192: Changing Time Period Filter](image)

**Configuring Axes**

The Left Axis is the independent axis because it is the first data collected. The Top Axis is dependent axis because it uses the Left Axis data as the data set.
The dependency occurs because the Log Investigator collects data that matches the Left Axis setting first; this data represents the data set for the entire log entry matrix. By default, the Left Axis is set to the data type Top Sources. After the Left Axis data set has been determined, the Log Investigator searches that data set for data that matches the Top Axis setting. By default, the Top Axis is set to the data type Top destinations.

Because the Left Axis setting controls the initial data set, it is the most important axis setting. Typically, you should set the Left Axis to the data type you most want to investigate.

Setting the Data Type
You can change the data type for each axis. The data type defines the type of information that the Log Investigator attempts to locate in your log entries. For either axis, you can set the following data types:

- **Top Sources**—The IP address that generated the event.
- **Top Destinations**—The IP address that received the event.
- **Top Subcategories**—The attack subcategory detected in the event.
- **Top Destination Ports**—The port numbers on the Destination device that received the event. The port number can help you identify the service used in the event.

By default, the Left Axis uses the data type Top Sources and the Top Axis uses the data type Top Destinations. To change these settings, select the desired data type in the data point source menu.

Setting Data Points
A data point is a single data type field that matches the axis setting. By default, each axis collects 10 data points for each evaluation. These default settings create a Log Entry Matrix of 100 cells (the top 10 source IP addresses are correlated against the top 10 destination IP addresses, creating a 100-cell matrix). For example, a data point count of 6 for each axis would create a 36-cell matrix.

You can set the data point higher (maximum 40) or lower (minimum 5), depending on your investigation requirements. To change these settings, select the desired data type in the data point count field. The higher the data count, the larger the log entry matrix—and the more processing power required by the Log Investigator UI. Using large data counts can slow performance.

**EXAMPLE: USING LEFT AND TOP AXES IN THE LOG INVESTIGATOR**
In this example, you configure swap the setting for the Left and Top Axes of the Log Investigator to see how each axis controls data.

Set the filter to Attacks, then configure the Left and Top Axes:

- To identify which of the most popular source addresses are generating attacks against the most popular destinations:
  - Select as the Left Axis (the independent axis) as Top Sources.
Select the Top Axis (the dependant axis) as Top Destinations. The Left Axis displays all attacks for the Top Source IP addresses, while the Top Axis displays the number of attacks for each of the Top Destinations attacked by the Top Sources.

To identify which of the most popular destination addresses are receiving attacks from the most popular sources:

- Select as the Left Axis (the independent axis) as Top Destinations.
- Select the Top Axis (the dependant axis) as Top Sources.

The Left Axis displays all attacks against the Top Destination IP addresses, while the Top Axis displays the number of attacks for each Top Source IP address that attacked a Top Destination.

Setting a Log Entry Limit

You can limit the number of log entries used in Log Investigator calculations. The NetScreen-Security Manager Device Server stores log entries from managed devices and the management system; when the GUI Server accesses a log entry to display its information in the UI, that log entry is placed in a log buffer. As the Log Investigator searches your log database for log entries that match the filter, time period, and data type criteria, it places all matching log entries in the log buffer.

To control the size of this buffer (the number of matching log entries), you can configure the Max Log Count for your investigations. The limit defines the number of matching log entries the Log Investigator accepts for its calculations.

You can set the following log entry limits:

- 100,000 log entries
- 200,000 log entries
- 400,000 log entries
- 600,000 log entries
- 800,000 log entries
- 1,000,000 log entries

Be aware that setting a large buffer limit can cause the Log Investigator performance to degrade. The maximum buffer size of one million log entries uses all memory on the GUI Server and is not recommended.

Setting Log Investigator Filters

Log Investigator filters operate very similar to Log Viewer filters: You set criteria for log entries and the Log Investigator filters out log entries that do not match the filter criteria. Using the Filter Summary dialog box, you can select and apply multiple filters to the Log Investigator matrix.
To set filters, from the file menu, select View > Set Filter. The following table details filter types:

Table 84: Log Investigator Filters

<table>
<thead>
<tr>
<th>Filter Type</th>
<th>Sample Filters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Filters</td>
<td>Time Received</td>
<td>Identifies packets by the time when a packet is sent from a device.</td>
</tr>
<tr>
<td></td>
<td>Time Generated</td>
<td>and when a packet is received on a device.</td>
</tr>
<tr>
<td>Address Filter</td>
<td>Source Address</td>
<td>Identifies packets based on information about an address of a device.</td>
</tr>
<tr>
<td></td>
<td>Destination Address</td>
<td>from which the packet was sent or an address of a device to which the packet is sent.</td>
</tr>
<tr>
<td></td>
<td>Device Address</td>
<td></td>
</tr>
<tr>
<td>Direction Filters</td>
<td>Inbound If</td>
<td>Identifies packets based on the direction they are heading to or from a specified device.</td>
</tr>
<tr>
<td></td>
<td>Outbound If</td>
<td></td>
</tr>
<tr>
<td>Device Filters</td>
<td>Device VIN</td>
<td>Identifies device ID number and virtual device value.</td>
</tr>
<tr>
<td></td>
<td>Virt Dev</td>
<td></td>
</tr>
<tr>
<td>Transmission Type Filters</td>
<td>Packets</td>
<td>Identifies transmissions based on whether they are seen as packets, bytes, or attacks.</td>
</tr>
<tr>
<td></td>
<td>Bytes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Attack</td>
<td></td>
</tr>
<tr>
<td>Port Filters</td>
<td>Src Port</td>
<td>Identifies packets based on the port on a device from where they were transmitted or on the port on a device to where they were transmitted.</td>
</tr>
<tr>
<td></td>
<td>Dst Port</td>
<td></td>
</tr>
<tr>
<td>Policy Filters</td>
<td>Policy ID</td>
<td>Identifies packets based on whether they meet the conditions of a policy or a rule.</td>
</tr>
<tr>
<td></td>
<td>Policy Version</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Rule Number</td>
<td></td>
</tr>
<tr>
<td>Alarm Filters</td>
<td>Flag</td>
<td>Identifies the severity level of a generated alarm.</td>
</tr>
<tr>
<td></td>
<td>Alarm</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td></td>
</tr>
<tr>
<td>Miscellaneous Filters</td>
<td>Protocol</td>
<td>Various</td>
</tr>
<tr>
<td></td>
<td>Category</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Email</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SNMP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Syslog</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td></td>
</tr>
</tbody>
</table>

**NOTE:** For a complete list of log entry columns available for filtering, see “Log Viewer Columns” on page 604.

After you have set a filter, the Filter Summary displays a list of all filters applied to the log entry data and the Log Investigator matrix displays values for matching log entries.
Using the Log Investigator

Chapter 14: Logging

Example: Setting Filters in the Log Investigator

In this example, the Left Axis is set to Top Sources and the Top Axis is set to Top Destination (these are the default settings). To set a filter that displays all attack category log entries generated by the Top Sources and received by the Top Destinations:

1. From the file menu, select View > Set Filter to display the Filter Summary dialog box.

2. In the filter list on the left, select Category, then select the following categories in the right: Predefined, Custom, and Screen.

3. Click OK to save and apply your changes.

To view the number of attacks between a specific source-destination pair, locate the Source Address 63.172.115.190 and Destination Address 63.172.115.6, then find the cell where the two addresses intersect. The Log Investigator displays 140 log entries for this Source-Destination pair, as shown below:

Figure 193: View Log Investigator Results

### Investigating Log Entry Data

After you have configured the Log Investigator options and set filters as desired, you are ready to begin investigating your log entry data.
Using Rows and Columns

Each row or column in the Log Entry matrix represents events for a single data type. When selecting a row/column, you are evaluating how the data type (source, destination, subcategory, or destination port) for that axis relates to the other axis during a specific time period. Typically, reviewing a row/column in the matrix helps you analyze all events for a single data type.

For example, to investigate a sudden drop in performance on a specific destination, set the Left Axis to Top Sources and the Top Axis to Top Destinations, then select the column for the destination IP address. For each cell that displays a high number of events received by that destination, locate the corresponding source IP address. You might determine that destination 1 is receiving a large number of events from source A, B, and C. This activity could be a harmless event, such as multiple users attempting to contact a single application server at the same time. You could eliminate the bottleneck by adding another application server to the network or restricting access to the existing server.

Using Cells

Each cell in the Log Entry matrix represents events that occur at the intersection of two data types. When selecting a cell, you are evaluating the events that occurred between those two specific data types (source, destination, subcategory, or destination port) during a specific time period. Typically, reviewing a cell in the matrix helps you analyze all events that occur between a data type pair.

For example, to investigate a sudden drop in network performance, set the Left Axis to Top Sources and the Top Axis to Top Destinations, then review the log entry matrix to locate a large number for a location pair. You might identify that source A is sending an unusually large number of transmissions to destination 1. This activity could be a harmless event, such as an employee archiving multiple large files before leaving work; however, this activity might be the result of a denial-of-service attack triggered by an internal trojan. You probably need to get more details, such as destination ports used and attack subcategories for the events before you can resolve the issue.

The following table details the benefits of each type of Log Investigator analysis.
You can zoom in on specific details about activity between two data types. You can select a third data type for comparison, or display details about the event over time. To get details, right-click a cell, row, or column and select Zoom In to see the list of available data types. Because the Zoom In menu is dynamic, it contains all data types not currently used for the Left or Top Axis of the Log Investigator matrix. Alternatively, you can select time as the third data type.

Details appear in the Zoom area, which contains two panes:

- The Zoom table (left pane)
- The Zoom chart (right pane)

The table and chart use the same information to generate values.

**EXAMPLE: VIEWING DESTINATION PORTS IN THE LOG INVESTIGATOR**

In this example, the Left Axis is set to Top Sources and the Top Axis is set to Top Destination (these are the default settings); the filter is set to attacks (for details on setting the filter, see “Setting Filters in the Log Investigator” on page 627).

To view the service ports on the destination device used by the attacks, right-click a cell that contains a non-zero value and select Zoom In > Dst Port. In the Zoom area:
The left pane displays a table of service ports listed in descending order (the port accessed by the most attacks is listed first). The left column lists the Destination Port Number and the right column lists the number of attacks received by that port number. Because services are mapped to specific port numbers, you can use the port number to identify the service used in the attack.

The right pane displays a chart using the same information.

**EXAMPLE: VIEWING SUBCATEGORY DETAILS IN THE LOG INVESTIGATOR**
In this example, the Left Axis is set to Top Sources and the Top Axis is set to Top Destination (these are the default settings); the filter is set to attacks (for details on setting the filter, see “Setting Filters in the Log Investigator” on page 627).

To view the individual attacks (the attack subcategories) against the destination device, right-click a cell that contains a non-zero value and select Zoom In > Subcategory. In the Zoom area, the left pane displays a table of attack subcategories listed in descending order (the attack found in the most number of log entries is listed first); the right pane displays a chart using the same information.

**EXAMPLE: VIEWING TIME PERIOD IN THE LOG INVESTIGATOR**
In this example, the Left Axis is set to Top Sources and the Top Axis is set to Top Destination (these are the default settings); the filter is set to attacks (for details on setting the filter, see the example “Setting Filters in the Log Investigator” on page 627).

To view the time period over which the attacks occurred, right-click a cell that has a non-zero value and select Zoom In > Time. In the Zoom area, the left pane displays a table of attacks listed in order (the oldest attack is listed first); the right pane displays a chart using the same information.

### Jumping to the Log Viewer

The Log Investigator uses log entry data for calculations, and does not display the actual log entries. However, you can use the Log Viewer to see the log entries used in Log Investigator calculations.

To see corresponding log entries, right-click a cell, row, or column from the Log Investigator matrix or the Zoom table and select View in Log Viewer. NetScreen-Security Manager creates a new UI window that displays the log entries in the Log Viewer.

### Excluding Data

You can manually configure the Log Investigator to exclude data for a cell, row, or column in the Log Investigator matrix. You might want to exclude:

- Irrelevant values (such as values from sources or destinations no longer in production)
- Abnormally high or low values (to establish a baseline)
- Specific data type (source, destination, destination port, subcategory)
High values (when investigating events that generate lower values)

To exclude a specific attack from the Log Investigator calculations, right-click the attack cell and select Exclude. To help you keep track of excluded values, the Filter Summary area displays a list of values you have manually excluded.

Using the Audit Log Viewer

The Audit Log Viewer monitors administrative events that occur when a NetScreen-Security Manager administrator makes changes to a domain. Use the Audit Log Viewer to track changes to your managed device configurations. You can view audit-log entries for all managed devices in the all domains you have access to, or you can view entries for the devices in a single domain. When the disk space reaches the defined usage, old audit log entries are purged.

The Audit Log Viewer appears as one of the modules in the NetScreen-Security Manager UI. Select the Audit Log Viewer to display the audit log entry table, device view, and target view, as shown in Figure 194:

![Audit Log Viewer UI Overview](image)

**NOTE:** You will see summaries in the Target Name or Device Name tables only for logs with targets and/or devices.
Audit Log Table

The audit log table contains the following columns of information shown in Figure 86.

Table 86: Audit Log Information

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Generated</td>
<td>The time the object was changed. The Audit Log Viewer displays log entries in order of time generated by Greenwich Mean Time (GMT).</td>
</tr>
<tr>
<td>Admin Name</td>
<td>The name of the NetScreen-Security Manager administrator who changed the object.</td>
</tr>
<tr>
<td>Admin Domain</td>
<td>The name of the domain (global or subdomain) that contains the changed object.</td>
</tr>
<tr>
<td>Operation Outcome</td>
<td>The final access-control status of activities is either success or failure.</td>
</tr>
<tr>
<td>Action</td>
<td>The type of change applied to the object. For a complete list of the actions that the Audit Log Viewer tracks, see “Audit Log Entry Actions” on page 633.</td>
</tr>
<tr>
<td>Target Object Type/Name/Domain</td>
<td>For changes made to a device configuration or object, the Audit Log Viewer displays the object type, an object name, and object domain.</td>
</tr>
<tr>
<td>Device Name/Type/Domain</td>
<td>For changes made to a device, the Audit Log Viewer displays the device name, object type, and device domain.</td>
</tr>
<tr>
<td></td>
<td>For changes made to the management system, such as administrator login/logout, the Audit Log Viewer does not display target or device data.</td>
</tr>
</tbody>
</table>

For changes to devices or device configurations, you can use the Target View and/or Device View to get more details about those changes.

Managing the Audit Log Table

NetScreen-Security Manager provides multiple ways to manage the data in your Audit Log table. The following sections describe these data-management options.

Select Audit Log Table

Use the Set Audited Activities option in the Edit menu to select read/write or read-only auditable activities. By default, all read/write activities are unchecked to avoid overloading the system’s storage capacity. The settings for selected activities are saved in GUI server and be used to decide whether to create audit-log entry for an activity.

Sort Audit Log Table

Sort one column at a time by clicking on the Time Generated, Admin Name, Command, or Operation Outcome columns. Sort one column at a time by clicking on column header. Hold down Ctrl key, mouse click on a column header to sort the selected column. Hold down Shift key, mouse click on a column header to clear sorting on the selected column. Arrow icon on table column header indicates descending or ascending order.

Filter Audit Log Table

Select or clear filters by right-clicking on the Time Generated, Admin Name, Admin Login Domain or Command columns. The types of filters are listed at the bottom of the window next to Filtered on. Adding and removing filters happen immediately.
Log Size and Data Migration

Once the disk space usage reached the defined threshold, the oldest audit log entries are purged before new entries are recorded. Configure the threshold in the guiSvr.cfg file.

You can migrate old audit log data into the latest version of the audit log.

Target View and Device View

The Audit Log Viewer also contains two detail views:

- **Target View**—For a change made to the device configuration, such as changing an IP address or renaming the device, select the audit log entry for that change in the audit log table, then view the Target View to see details about that change.

- **Device View**—For a change made to the device itself, such as adding the device, autodetecting a device, or rebooting a device, select the audit log entry for that change in the audit log table, then view the Device View to see details about that change.

To see additional details for a target or device audit log entry, double-click the entry in the Target or Device View. For targets, NetScreen-Security Manager displays the configuration screen that the change was made in and marks the changed field with a solid green triangle. For devices, NetScreen-Security Manager displays the Job Manager information window for the job task.

Setting a Start Time for Audit Log Entries

By default, the Audit Log Viewer displays audit log entries in order of time generated by Greenwich Mean Time (GMT). To configure the Audit Log Viewer to display log entries for events that occurred after a specific time, configure the Log By Time option.

From the menu bar, select View > Go To Log By Time to display the Log By Time dialog box. Select a date and time, then click OK to save and apply the time change to the Audit Log Viewer. The audit log table now displays only the audit log entries that were generated on or after the date and time you specified.

Audit Log Entry Actions

The Audit Log records the following administrative actions:

- Access control denied
- Auto detect vsys
- Add device
- Autodetect device
- Configuration verification
- Delete certificate
- Delete device
- Delete object
- Delete vsys device
- DI attack check
- DI attack update
- DNS refresh
- Download running configuration
- Failover revert
- Failover status
- Flash synchronization
- Generate certificate
- Generate preshared key
- Get configuration summary
- Get delta configuration summary
- Get license key info
- Get running configuration summary
- Get rule validation summary
- Get policy list
- Import cluster member
- Import configuration
- Import configuration offline
- Import vsys device
- Insert object
- Install software key
- Modify BGP peer session
- NTP update
- Policy merge
- Reboot device
- Refresh certificate list
Managing Log Volume

Security administrators have different requirements for how many log entries they need to keep. Some administrators must keep all log entries as directed by their corporate Security Policy, resulting in large numbers of log entries that the administrator might not have time to review, but need to store.

To manage log volume, you can use the NSM UI to both archive and purge logs.

**NOTE:** Excessive logging creates additional traffic on your network. It is recommended that you balance your logging needs with the performance needs of your management system.

You can also export your log records to other formats for use in other applications. For details on how to forward logs, see “Forwarding Logs” on page 639.

### Archiving Logs

You can archive and retrieve log entries to and from a storage device using standard Unix commands.

Logs reside on the Device Server in the following directory:

```
/usr/netscreen/DevSvr/var
```

We recommend using the following commands to archive your logs:

- The `tar` command
The `scp` (Secure Copy) command

The `ftp` (File Transfer Protocol) command

For full descriptions and options for each command, see the man pages.

**NOTE:** You do not need to stop the processes on the Device Server before archiving.

### Purging Logs

The Device Server maintains a minimum of 1000Mb (by default) of disk space available, primarily for the storage of log records. When the available disk space reaches this minimum, it sends an email alerting you of the situation.

**NOTE:** Use the Server Manager node in the NetScreen-Security Manager UI to configure email notification. Refer to “Configuring Servers” on page 552 for more information.

In the event that disk space on the Device Server reaches a minimum of 500Mb, the Device Server attempts to free the disk space by purging log records beginning with the oldest records on file. The Device Server stops purging log records when the 1000Mb minimum disk space is restored. If for any reason, the Device Server is not able to restore 500Mb of disk space, the Device Server will automatically shut down. If the Device Server fails to restart for this reason, an error message appears in the console window indicating that there is not enough disk space on the server machine, and that you must either backup your data or free up additional disk space in order to start the server again.

If you want to change the parameters for managing disk space on the Device Server, you can edit the Device Server configuration file. For more information on configuring the minimum disk space available on the Device Server, refer to the NetScreen-Security Manager Installer’s Guide.

### Managing Logs

In NetScreen-Security Manager, logs are gathered and stored by the Device Server. In a given deployment, the Device Server may be deployed on the same machine as the GUI Server or on a separate machine. When determining the disk space requirements for NetScreen-Security Manager, the log management strategy must be considered. The Device Server has the most variability on disk space requirements.

**Automatic Device Log Cleanup**

There is an automatic mechanism built into NetScreen-Security Manager for managing disk space which cleans up old logs when the available disk space falls below a specified threshold. The log cleanup parameters are determined in the `/var/netscreen/DevSvr/devSvr.cfg` file. There are three settings in this file that pertain to log management:

1. `storageManager.minimumFreeSpace`: determines when a warning will be generated indicating low remaining disk space. The default value is 200 MB.
2. **storageManager.threshold**: determines when the system will begin to clean up the oldest log files in order to return to the storageManager.minimumFreeSpace setting. The default value is 100 MB.

3. **statusMonitor.updateInterval**: determines the frequency with which the system checks the available disk space.

   The default value is 3000000 microseconds (3 seconds).

   With the default settings, NetScreen-Security Manager will generate an alert when the free disk space reaches 200 MB. It will begin deleting the oldest logs when the system reaches 100 MB free disk space and continue deleting until 200 MB of disk space is available.

**Log Archival Mechanism**

All managed device logs are stored in `/usr/netscreen/DevSvr/var/logs`. In that directory there is a directory for each day. The log and associated files for that day are within that directory. In order to archive the logs for a specified day, the entire directory should be archived together.

Each directory takes the name YYYYMMDD, indicating which day is contained in the directory. Archival should not be attempted on the current day’s files. You can automate this using cron. Use the following procedure as a suggested process for automatically archiving the logs.

1. Use `scp` to copy all directories in `/usr/netscreen/DevSvr/var/logs/` that are earlier than desired archival date (< YYYYMMDD) to remote archival location.

2. Remove directories from Device Server machine.

   At some later time, you can analyze the archived logs by restoring them to the logs directory on the Device Server. Once restored to this directory, the logs will be available in the Log Viewer and Log Investigator just as they were before archival.

   1. Use `scp` to copy directories from remote archival location to `/usr/netscreen/DevSvr/var/logs/`

   2. Analyze using NSM UI

   3. Remove directories when finished with analysis.

**Setting Log Storage Limits**

You can specify the number of days NSM will store logs as well as purge or archive a specified log based on one of the following configurable criteria:

- Date Limits
- System-Wide Retention Policy
- Obsolete Logs
- Required Disk Space
Date Limits
If you use a date to purge or archive logs, the limit is based only on the calendar date.

System-Wide Retention Policy
The system administrator can specify the maximum number of days the system stores logs. One configuration throughout NSM is permitted at a time. Users can specify how the retention policy is triggered and when it is scheduled.

Obsolete Logs
As logs become obsolete, the user can archive before the system purges the logs. You have the option of purging the logs directly or archiving them first. If you select the archive option, NSM archives all the logs from the selected date.

Required Disk Space
After defining the number of logs and the number of days you want archived, NSM estimates the disk space required for storing the logs. In calculating the estimated required disk space, NSM uses the average size of logs per day and will indicate to the user how the estimate was reached or if there was not data available to provide an estimate.

Archive Location
The location of the archive is user-configurable from the Disk and Log Management dialog box. The options are Local and Remote.

Local—To archive logs locally, specify the directory location where the files will be stored in the Archive Location field.

Remote—To archive logs remotely, specify the IP address, username, password, and the protocol (scp and sftp). The path on the remote server will be stored in the user preferences. SCP and SFTP work only with trusted hosts.

File Name
One log archive location is applicable throughout the system. The following naming convention is used for storing the log files:

```
YYYYMMDD_<No>.tar.gz
```

where:
YYYYMMDD is the date of the file containing the log
No is the archive number if multiple archival for the same date.

NOTE: If the archive process fails, (for instance if the host is not preconfigured or if there is not enough disk space) the user is notified via email and NSM creates an error log entry. However, the selected logs will still be purged even if the archival fails.
Define Location
Before you archive a log, you must first define the location of the archived log. To do this, open NSM and select Server Manager > Servers > Device Server > Disk and Log management. Enter the following path in the Archive Location text box where NSM creates the archives file.

/usr/netscreen/DevSvr/var/devSvr.cfg

Forwarding Logs
You can forward your log records for use in other applications using one of the following methods:

- **Action Manager**—use the Action Manager, a node on the main UI, to configure the management system to forward logs generated within a specific domain or subdomain in NetScreen-Security Manager.

- **Log2Action utility**—a command line utility located on the NetScreen-Security Manager Device Server.

NOTE: You can also forward logs based on specific rules in a security policy. Refer to Configuring Firewall Rules on page 330 for more information.

Sending Email Notification of Downed Device
You can configure NetScreen-Security Manager to send you an email notification when a device goes down so that even if you do not have access to NetScreen-Security Manager, you will be informed of device status.

1. In the main navigation tree, click Action Manager > Action Parameters, then double-click the row that lists all your action parameters.

2. Enter the default email address in the E-Mail section for the ‘From’ email address.

3. Click the Add icon to open the New Add/Edit E-Mail Address dialog box.

4. Enter the default ‘To’ email address for all log actions in the current domain, then click OK. Repeat this step if additional default ‘To’ email addresses are required.

5. In the main navigation tree, click Action Manager > Device Log Action Criteria, then click the Add icon.

6. Click the Category drop-down list box and select Info, select the Device Disconnect subcategory, then click OK to save the changes.

7. Click the Actions tab, check SMTP Enable.

8. Configure the target email address(es) for this rule, if they differ from the defaults you configured in the previous steps.
Using the Action Manager to Forward Logs by Domain

Use the Action Manager node to configure the management system to perform actions (such as syslog, export, or alarm) on log data based on the criteria you specify. These actions occur for all the managed security devices in a specific domain or subdomain.

To enable the management system to export logs, you must configure the following:

- **Action Parameters**—These settings define the default log export settings for the management system, and determine how the system handles qualified log entries (log entries that match specified log criteria).

- **Device Log Action Criteria**—The criteria specifies the category and severity of the log entries you want to export. When a log entry meets the specified criteria, it is considered qualified, and NetScreen-Security Manager performs the specified actions defined in the criteria.

Configuring Action Parameters

From the Action Manager, select Action Parameters to define the default log export settings for the management system. To enable the management system to export qualified logs to Syslog, SNMP, CSV, XML or email, configure the export settings for each format as detailed in the following sections.

**Exporting to Syslog**

For exporting to syslog, configure the IP address and the server facility for the syslog server to which you want to send qualified logs. NetScreen-Security Manager uses this server when exporting qualified log entries to syslog.

This setting defines the syslog settings for the management system. To actually export logs to the syslog server, you must select “Syslog Enable” using the Actions tab in the Device Log Action Criteria node.

**Exporting to SNMP**

For exporting to SNMP, configure the following SNMP settings:

- **SNMP Manager**—Specify the IP address of the SNMP server to which the GUI Server sends SNMP traps.

- **SNMP Community**—Specify an SNMP community name that provides a desired combination of both read and write access from the SNMP server.

NetScreen-Security Manager uses this information when exporting qualified log entries to SNMP. This setting defines the SNMP settings for the management system. To actually export logs to the specified SNMP server and community, you must select “SNMP Enable” using the Actions tab in the Device Log Action Criteria node.

**NOTE:** The NSM MIB files reside in the /usr/netscreen/DevSvr/utils directory on the management system. The file names are jnx-nsm-traps.mib and jnx-smi.mib.
Exporting to CSV
For exporting to CSV, configure the following CSV settings:

- **File Path**—The directory and filename that you want log entries exported to in .CSV format.
- **Print Header**—When selected, column headers are exported to .CSV format.

NetScreen-Security Manager uses this information when exporting qualified log entries to CSV. This setting defines the CSV settings for the management system. To export logs to CSV, you must select “CSV Enable” using the Actions tab in the Device Log Action Criteria node.

Exporting to XML
For exporting to XML, configure the directory and filename to which you want to send qualified logs in XML format. NetScreen-Security Manager uses this information when exporting qualified log entries to XML; each log becomes an XML record, which you can open in most Web browsers.

This setting defines the XML settings for the management system. To actually export logs to XML, you must select “XML Enable” using the Actions tab in the Device Log Action Criteria node.

Exporting to Email
For exporting to email, configure the following email and SMTP settings:

- **SMTP Enable**—Enables the SMTP server to send email.
- **Default ‘From’ Email Address**—Some servers require a valid “from” email address” to relay mail.
- **Default ‘To’ Email Addresses**—The email address that receives email alarms. You can specify multiple “to” email addresses.

NetScreen-Security Manager uses this information when exporting qualified log entries to email. This setting defines the email and SMTP settings for the management system.

NOTE: After editing your email settings, you must restart the Device Server for your changes to take effect.

Setting Device Log Action Criteria
A Device Log Action Criteria instance defines the criteria for a qualified log; each instance contains two criteria settings (category and severity), and multiple action settings for logs that meet the criteria settings. For example, to only export critical severity attack logs to XML, you create a device log action criteria instance that specifies the log category as predefined, the severity as critical, and the action as XML. For each log entry that matches the criteria, NetScreen-Security Manager exports the log as XML, using the default XML settings configured in the Actions tab.
To add a new Device Log Action Criteria instance, use the Add button, then configure the following settings.

Selecting Category
In the Category list, select a category of log entry for the criteria. Some categories contain subcategories; however, to set an action based on a subcategory, you must first select a category.

For details on each category and subcategory, see Appendix E, “Log Entries”.

Selecting Severity
In the Severity tab, select the severities for the criteria.

Selecting Actions
In the Actions tab, select the actions (SNMP, syslog, XML, CSV, Email, and Script) you want the management system to take for logs that meet the criteria. You can enable multiple actions.

When you enable the Email/SMTP and Script actions, you can also configure the following additional settings:

- Email Action—To direct the management system to email qualified log records, specify the From and To email addresses:
  - From Email Address—The email address that the server uses to send email. Some servers require a valid “from” email address to relay mail.
  - To Email Addresses—The email address that receives email alarms. You can specify multiple “to” email addresses.

- Script Action—To direct the management system to send qualified log records to a script, you must configure the following:
  - Script Enable
  - Script To Run—Select the script you want to run from the Script To Run list. For a script to appear in the list, the script must be located in the appropriate directory on the NetScreen-Security Manager Device Server. The appropriate directory is as follows:
    - Scripts for the global domain must appear in 
      /usr/netscreen/DevSvr/lib/scripts/
      By default, this directory contains two sample scripts, sample.sh and sample.pl.
    - Scripts for subdomains must appear in 
      /usr/netscreen/DevSvr/var/subDomainName/
      where subDomainName is the name of the subdomain. The subDomainName directory must be created manually.
  - Action Upon Script Failure—Specify the error handling for the script:
- Skip. Directs the system to skip any log for which the script had an error.

- Retry. Directs the system to try the action again for the same log. When using this filter, you must also specify:
  - Retry Count. Specifies the maximum number of retries to attempt before moving on to the next log record.
  - Retry Interval (in seconds). Specifies the number of seconds until the action is tried again.

**Using the Log2Action Utility to Export Logs**

You can also use a command line utility on the Device Server to export logs. To export to XML, CSV, SNMP, Syslog, email, or script format using the Log2Action utility:

1. Log in to the NetScreen-Security Manager Device Server as root.
2. Change to the utility directory by typing: `cd /usr/netscreen/DevSvr/utils`
3. Specify the common filters, format, and format-specific filters for the format you want to export to:

   ```
   sh devSvrCli.sh --log2action <common_filters> --action <format> <format_options>
   ```

   The log2action utility exports all log records to the specified format. After executing the action, the system generates an exit status code of 0 (no errors) or 1 (errors).

   The following sections detail common filters, actions, and required and optional format-specific filters.

**Using Filters**

The log2action utility generates data for a maximum of 100,000 logs.

---

**NOTE:** If you want to generate more than 100,000 logs, use the matches-to-return option to specify the number of logs that you want.

---

Because of the large volume of logs potentially generated, it is highly recommended that you specify filtering criteria when using the log2action utility. Without filtering, the action report generates data from the earliest date in the log database and stops providing output after 100,000 logs. In this case, it is possible that you may not get the action output of your most recent data. Specifying a time filter is recommended in this situation.

**Using Time Filters**

For example, if you wanted to view data in the logs of 20060317, run the following command:

```
./devSvrCli.sh -log2action -filter -log-id 20060317:0-20060317:4294967294
-action --xml --file-path /tmp/newtest.xml
```
If you wanted to view data for all logs from 20060315 to 20060317, run the following command:

```bash
./devSvrCli.sh -log2action -filter -log-id 20060315:0-20060317:4294967294
-action --xml --file-path /tmp/newtest.xml
```

### Using Common Filters

To control which log records are exported, use common filters. Common filters are optional and must be used before the action command (`--action`).

The following common filters display:

<table>
<thead>
<tr>
<th>Option</th>
<th>Default</th>
<th>Multiple</th>
<th>Specifies</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>--domain</td>
<td>*</td>
<td>yes</td>
<td>Domain path</td>
<td><code>&lt; global[/&lt; subdomain-name&gt;]</code></td>
</tr>
<tr>
<td>--src-ip</td>
<td>*</td>
<td>yes</td>
<td>Source IP address</td>
<td>`&lt; a.b.c.d[/n</td>
</tr>
<tr>
<td>--dst-ip</td>
<td>*</td>
<td>yes</td>
<td>Destination IP address</td>
<td>`&lt; a.b.c.d[/n</td>
</tr>
<tr>
<td>--src-port</td>
<td>*</td>
<td>yes</td>
<td>Source port</td>
<td><code>&lt;[0-65535][0-65535]&gt;</code></td>
</tr>
<tr>
<td>--dst-port</td>
<td>*</td>
<td>yes</td>
<td>Destination port</td>
<td><code>&lt;[0-65535][0-65535]&gt;</code></td>
</tr>
<tr>
<td>--matches-to-return</td>
<td>no</td>
<td></td>
<td>Number of log entries to match</td>
<td><code>&lt;[1-100000]&gt;</code></td>
</tr>
<tr>
<td>--log-id</td>
<td>*</td>
<td>no</td>
<td>From Log ID to To Log ID</td>
<td><code>&lt; &lt; yyyy-mm-dd&gt;:&lt;0-MAX&gt;[:&lt; yyyy-mm-dd&gt;:&lt;0-MAX]&gt;</code></td>
</tr>
<tr>
<td>--time-recv</td>
<td>*</td>
<td>yes</td>
<td>Time received</td>
<td><code>&lt; &lt; yyyy-mm-dd&gt;:&lt;hh:mm:ss&gt; &gt; &lt; &lt; yyyy-mm-dd&gt;:&lt;hh:mm:ss&gt;</code></td>
</tr>
<tr>
<td>--severity</td>
<td>*</td>
<td>yes</td>
<td>Severity</td>
<td><code>&lt; severity&gt;</code></td>
</tr>
<tr>
<td>--user-flag</td>
<td>no</td>
<td>yes</td>
<td>User flag number</td>
<td><code>&lt;[0-7]&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>High = 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Medium = 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Low = 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Closed = 3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>False Positive = 4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Assigned = 5</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Investigate = 6</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Follow-Up = 7</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Pending = 8</td>
</tr>
<tr>
<td>--rule</td>
<td></td>
<td></td>
<td>Rule to match</td>
<td>`&lt; domain-path&gt;:&lt; policy-name&gt;:&lt; rulebase (fw</td>
</tr>
<tr>
<td>--category</td>
<td>*</td>
<td>yes</td>
<td>Category</td>
<td><code>&lt; category&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(self, config, traffic, alarm, info, predefined, custom, screen, implicit)</td>
</tr>
<tr>
<td>--action</td>
<td>*</td>
<td>no</td>
<td>Action, usually followed by format-specify filters</td>
<td><code>&lt; action&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(csv, email, script, snmp, sylog, xml)</td>
</tr>
</tbody>
</table>
Some common filters support multiple entries, enabling you to specify more than one criteria. When using multiple entries for a common filter, you must use the common filter before each entry.

**NOTE:** Use -help to print all relevant filter options.

### Using Format-Specific Filters

To control how log records are exported, use format-specific filters. Some formats have required and optional format-specific filters.

**NOTE:** Variable data is only exported in .csv format.

Use format-specific filters after the specified action. To see all format-specific filters for a format, type:

```
sh devSvrCli.sh --log2action --action --format
```

### Exporting to XML

The xml action directs the system to output logs using the XML format. To export:

1. Login to the Device Server as root, then change to the utility directory by typing:
   
   ```
cd /usr/netscreen/DevSvr/utils
   ```

2. To export to a file, type:

   ```
   sh devSvrCli.sh --log2action --action --xml <file-path> <include-header>
   ```

The Device Server exports all log records to XML; each log record becomes an XML record, which you can open in most Web browsers.

### Using XML Required/ Optional Format-Specify Filters

You can use the following required and optional format-specific filters for exporting to XML:

<table>
<thead>
<tr>
<th>CSV</th>
<th>Multiple</th>
<th>Required</th>
<th>What It Means</th>
</tr>
</thead>
<tbody>
<tr>
<td>--file-path</td>
<td>No</td>
<td>Yes</td>
<td>Specifies where the system should direct the output. For example, myLogs.xml</td>
</tr>
<tr>
<td>--include-header</td>
<td>No</td>
<td>No</td>
<td>Specifies that the system should print the field name before each field.</td>
</tr>
</tbody>
</table>

### Viewing XML Format Output

To view the XML schema file, type:

```
/usr/netscreen/DevSvr/lib/logActions/log.xsd
```
EXEMPLARY: EXPORTING ATTACK CATEGORY LOG RECORDS TO XML
To export predefined and custom attack category log records to an XML file located in the /usr directory of the Device Server, use the --category common filter to specify the categories:

```
sh devSvrCli.sh --log2action --category predefined --category custom --action --xml --file-path /usr/MyXmlLogRecords/attacks.xml
```

Exporting to CSV
The csv action directs the system to output logs using the CSV format. To export:

1. Login to the Device Server as root, then change to the utility directory by typing: cd /usr/netscreen/DevSvr/utils.

2. To export to a file, type:

```
sh devSvrCli.sh --log2action --action --csv <file-path> --include-header
```

The Device Server exports all log records to CSV; each log record becomes an CSV record.

Using CSV Required/Optional Format-Specify Filters
You can use the following required and optional format-specific filters for exporting to CSV:

<table>
<thead>
<tr>
<th>CSV</th>
<th>Multiple</th>
<th>Required</th>
<th>What It Means</th>
</tr>
</thead>
<tbody>
<tr>
<td>--file-path</td>
<td>No</td>
<td>Yes</td>
<td>Specifies where the system should direct the output. For example, myLogs.csv</td>
</tr>
<tr>
<td>--include-header</td>
<td>No</td>
<td>No</td>
<td>Specifies that the system should print the field name before each field.</td>
</tr>
</tbody>
</table>

Viewing CSV Format Output
CSV log files use this format:

Log Day Id, Log Record Id, Time Received (UTC), Time Generated (UTC), Device Domain, Device Domain Version, Device Name, Device IpAddr, Category, Sub-Category, Src Zone, Src Intf, Src Addr, Src Port, NAT Src Addr, NAT Src Port, Dst Zone, Dst Intf, Dst Addr, Dst Port, NAT Dst Addr, NAT Dst Port, Protocol, Policy Domain, Policy Domain Version, Policy, Rulebase, Rule Number, Action, Severity, Is Alert, Details, User, App, URI, Elapsed Secs, Bytes In, Bytes Out, Bytes Total, Packets In, Packets Out, Packets Total, Repeat Count, Has Packet Data, Var Data Enum

EXEMPLARY: EXPORTING COLUMN HEADERS TO CSV
To print the column headers for log records when exporting to a CSV file, use the include-header option:

```
sh devSvrCli.sh --log2action --action --csv --include-header --file-path /usr/MyCSVLogRecords/logrecords.csv
```
Exporting to SNMP

The snmp action directs the system to output logs to an snmp server in snmp format. You must specify the SNMP community string and the SNMP server IP address that receives the exported log records.

To export:

1. Login to the Device Server as root, then change to the utility directory by typing: `cd /usr/netscreen/DevSvr/utils`

2. To export to a file, type:
   ```
   sh devSvrCli.sh --log2action --action --snmp <community> <server>
   ```

   The Device Server exports all log records to the specified SNMP community and server.

Using SNMP Required/Optional Format-Specify Filters

You can use the following required format-specific filters for exporting to SNMP:

<table>
<thead>
<tr>
<th>SNMP</th>
<th>Multiple</th>
<th>Required</th>
<th>What It Means</th>
</tr>
</thead>
<tbody>
<tr>
<td>--community</td>
<td>No</td>
<td>Yes</td>
<td>Specify SNMP community string. For details on the community parameter, refer to section 3.2.5 of RFC 1098 for. You might need to ask your SNMP server administrator for the server community string.</td>
</tr>
<tr>
<td>--server</td>
<td>No</td>
<td>Yes</td>
<td>Specify SNMP manager IP address</td>
</tr>
</tbody>
</table>

The SNMP format has no optional format-specific filters.

Viewing SNMP Format Output

SNMP trap log entries use the following format:

```
<day id>-<record id> <timestamp> <sensor addr> <src addr>:<src port> <dst addr>:<dst port> <nat src addr>:<nat src port> <nat dst addr>:<nat dst port> <user> <in nic> <out nic> <sensor vin> <virtual dev> <attack> <policy name>:<policy ver> <rulebase> <rule number> <bytes> <packets> <elapsed> <protocol> <category>-<subcategory> <action> <session id1>-<session id2> <is hidden> <is duplicate> <is alert> <severity> <run script> <send email> <send snmp> <send syslog>
```

EXAMPLE: EXPORTING TO A SNMP SERVER

To send log records to the public SNMP server at 192.168.1.15, use the --public and --server options:

```
sh devSvrCli.sh --log2action --action --snmp --community public --server 192.168.1.15
```
Exporting to Email

The email action directs the system to output logs to an email address in SMTP format. You must specify the recipient email address that receives the exported log records and, optionally, the sender email address.

To export:

1. Login to the Device Server as root, then change to the utility directory by typing: `cd /usr/netscreen/DevSvr/utils`

2. To export to a file, type:

   `sh devSvrCli.sh --log2action --action --email <sender> <recipient>`

The Device Server exports all log records to the specified email address for the recipient.

**NOTE:**
You do not specify the SMTP server IP address in the log2action utility. The system uses the IP address configured for email in the Log Actions area of the GUI Server (in the NetScreen-Security Manager UI). For details on configuring this value, see “Exporting to Email” on page 641. You must configure the IP address before attempting to export logs to an email address.

Using Email Required/Optional Format-Specify Filters

You can use the following required and optional format-specific filters for exporting to email:

<table>
<thead>
<tr>
<th>SMTP</th>
<th>Multiple</th>
<th>Required</th>
<th>What It Means</th>
</tr>
</thead>
<tbody>
<tr>
<td>--recipient</td>
<td>Yes</td>
<td>Yes</td>
<td>Specify the receiving email address for the SMTP log records</td>
</tr>
<tr>
<td>--sender</td>
<td>No</td>
<td>No</td>
<td>Specify the sender email address</td>
</tr>
</tbody>
</table>

Exporting to syslog

The syslog action directs the system to output logs to a syslog server in syslog format. You must specify the IP address of the syslog server that receives the exported log records and the syslog facility.

To export:

1. Login to the Device Server as root, then change to the utility directory by typing: `cd /usr/netscreen/DevSvr/utils`

2. To export to a file, type:

   `sh devSvrCli.sh --log2action --action --syslog <server> <facility>`

The Device Server exports all log records to the specified IP address for the syslog server.
Chapter 14: Logging

Using Syslog Required/Optional Format-Specify Filters

You can use the following required format-specific filters for exporting to syslog:

<table>
<thead>
<tr>
<th>Filter</th>
<th>Multiple</th>
<th>Required</th>
<th>What It Means</th>
</tr>
</thead>
<tbody>
<tr>
<td>--server</td>
<td>No</td>
<td>Yes</td>
<td>Specify syslog server IP address as [IP</td>
</tr>
<tr>
<td>--facility</td>
<td>Yes</td>
<td>Yes</td>
<td>Specifies the facility that receives syslog messages. For details on the facility parameter, refer to section 4.1.1 of RFC 3164. The syslog severity, also used to calculate the overall syslog message priority, is automatically set to alert.</td>
</tr>
</tbody>
</table>

The syslog format has no optional format-specific filters.

Viewing Syslog Format Output

Syslog messages use the following format:

<day id>, <record id>, <timeReceived>, <timeGenerated>, <domain>, <domainVersion>, <deviceName>, <deviceIpAddress>, <category>, <subcategory>, <src zone>, <src intface>, <src addr>, <src port>, <nat src addr>, <nat src port>, <dst zone>, <dst intface>, <dst addr>, <dst port>, <nat dst addr>, <nat dst port>, <protocol>, <rule domain>, <rule domainVersion>, <policyName>, <rulebase>, <rule number>, <action>, <severity>, <is alert>, <details>, <user str>, <application str>, <uri str>, <elapsed>, <bytes in>, <bytes out>, <bytes total>, <packet in>, < packet out>, < packet total>, <repeateCount>, <hasPacketData>, <varData Enum>

Exporting to a Script

The script action directs the system to execute a script, use STDIN to pass log records formatted as XML to the script, and report output status. You must specify the name of the script that receives the exported log records (script must be located in the /usr/netscreen/DevSvr/lib/scripts/ directory).

To export:

1. Login to the Device Server as root, then change to the utility directory by typing: cd /usr/netscreen/DevSvr/lib.

2. To export to a file, type:

   sh devSvrCli.sh --log2action --action --script <script-name> <error-handling>

The Device Server exports all log records to the specified script.

Using Script Required/Optional Format-Specify Filters
You can use the following required format-specific filters for exporting to a script:

<table>
<thead>
<tr>
<th>Script</th>
<th>Multiple</th>
<th>Required</th>
<th>What It Means</th>
</tr>
</thead>
</table>
| --script-name  | No       | Yes      | Specify script name. The script must be located in the
|                |          |          | /usr/netscreen/DevSvr/lib/scripts/<domain>/<script-name>                      |
|                |          |          | For example:                                                                  |
|                |          |          | /usr/netscreen/DevSvr/lib/scripts/global/<script-name>                       |
|                |          |          | or                                                                            |
|                |          |          | /usr/netscreen/DevSvr/lib/scripts/global/<subdomain>/<script-name>           |

<table>
<thead>
<tr>
<th>--error-handling</th>
<th>No</th>
<th>Yes</th>
<th>Specifies error handling for the specified script. When using this filter, you must specify one of the following error-handling filters:</th>
</tr>
</thead>
</table>
|                  |      |       | ■ --skip 
|                  |      |       | Directs the system to skip any log for which the script had an error.       |
|                  |      |       | ■ --retry 
|                  |      |       | Directs the system to try the action again for the same log. When using this filter, you must also specify: |
|                  |      |       | ■ --retry-interval
|                  |      |       | Specifies the number of seconds until the action is tried again.            |
|                  |      |       | ■ --num-retries
|                  |      |       | Specifies the maximum number of retries to attempt before moving on to the  |
|                  |      |       | next log record.                                                            |

The script format has no optional format-specific filters.
Use the Report Manager module in Juniper Networks NetScreen-Security Manager to generate and view reports summarizing log and alarms generated by the managed Juniper Networks security devices in your network. You can use these reports to track and analyze log incidents, network traffic, and potential attacks.

This chapter contains the following sections:

- About Reporting on page 652
- Report Types on page 653
- Setting Report Options on page 663
- Log Viewer Integration on page 665
- Using Reports on page 667
- Using Statistical Reports on page 672
- Using the Watch List on page 672
About Reporting

The Report Manager module in NetScreen-Security Manager is a powerful and easy-to-use tool that enables you to generate reports summarizing key log and alarm data originating from the managed devices in your network. The reports in Report Manager provide a useful complement to the monitoring and logging capabilities in NetScreen-Security Manager enabling you to track and analyze network traffic, activities, and potential attacks.

Report Manager contains the following benefits for generating reports:

- Report Type Groupings
- Graphical Data Representation
- Integration with Logs
- Central Access to Management Information

Report Type Groupings

The reports in Report Manager are grouped together according to the type of data they provide:

- FW/VPN—Series of reports summarizing log and alarm data generated by the managed security devices in your network.
- DI/IDP—Includes reports that provide data on deep inspection and intrusion detection and prevention attacks.
- Screen—Includes reports that provide data on Screen attacks detected by the firmware on the managed security devices in your network.
- Administrative—Includes reports specifically designed to help system administrators track and manage log incidents and security rules.
- UAC Reports—includes reports that provide data on Unified Access Control (UAC) sessions.
- My Reports—Includes all reports that you have saved or created as a custom report.
- Shared Reports—Includes all reports that you have saved or created that you want made accessible to others in a domain.

Grouping these reports by type enable administrators and operations staff interested in tracking and analyzing specific types of information need to work only within the group of reports that they need.

For details on each of the specific reports per group, see “Report Types” on page 653. For additional details on each report type grouping, refer to the NetScreen-Security Manager Online Help.
Graphical Data Representation

You can use reports to view log data in both tabular and graphical form. The various depictions of the data make it easier to identify trends and potential areas of risk. Depending on your preference, you can also choose to view the data in either a horizontal bar graph or a pie chart.

Integration with Logs

Reports are also integrated with the Log Viewer and Log Investigator modules. By clicking a data point depicted in a report, you can quickly drill down to access and view the specific log entries presented in the report data. Refer to “Log Viewer Integration” on page 665 for more information about how you can use reports and log entries together to further analyze network events and attacks.

Central Access to Management Information

For network administrators and security analysts interested in tracking and identifying potential network trends and attacks, Report Manager provides a single graphical view into the network.

Report Types

Report Manager contains a set of predefined reports that you can use out of the box. It is recommended that you use the predefined reports first to familiarize yourself with how reporting works in NetScreen-Security Manager. You can then later fine tune these reports by generating custom reports based on the predefined reports.

Predefined Reports

The predefined reports in Report Manager provide a summary of key log events and alarms generated by the devices in your network (such as Top Scan Sources or Top Attacks). Two reports (Logs By User-set Flag and Top Rules) provide administrative information useful if you are tracking incidents or optimizing your rules. For typical use cases describing each of these reports, see “Using Reports” on page 667.

For your convenience, Report Manager groups predefined reports into the following categories:

- Firewall/VPN Reports
- DI/IDP Reports
- Screen Reports
- Administrative Reports
- UAC Reports

Firewall/VPN Reports

Table 88 lists and describes reports in NetScreen-Security Manager that provide information related to your network’s firewalls and VPNs.
Table 88: Firewall and VPN Reports

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Alarms</td>
<td>The total number of alarms generated by the managed security devices in your network, excluding traffic alarms.</td>
</tr>
<tr>
<td>Top Traffic Alarms</td>
<td>The total number of traffic alarms generated by the managed security devices in your network.</td>
</tr>
<tr>
<td>Top Traffic Log</td>
<td>The total number of traffic log entries generated by the managed security devices in your network, within filter constraints.</td>
</tr>
<tr>
<td>Top Configuration Logs</td>
<td>The total number of configuration log entries generated by the managed security devices in your network, within filter constraints.</td>
</tr>
<tr>
<td>Top Information Logs</td>
<td>The total number of information log entries generated by the managed security devices in your network, within filter constraints.</td>
</tr>
<tr>
<td>Top Self Logs</td>
<td>The total number of Self log entries generated by the managed security devices in your network, within filter constraints.</td>
</tr>
</tbody>
</table>

DI/IDP Reports

The following table lists and describes reports in NetScreen-Security Manager that provide deep inspection and intrusion detection and prevention information.

Table 89: DI/IDP Reports

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top 100 Attacks (last 24 hours)</td>
<td>Those attacks that are detected most frequently within the last 24 hours.</td>
</tr>
<tr>
<td>Top 100 Attacks Prevented (last 24 hours)</td>
<td>Those attacks that are prevented most frequently within the last 24 hours.</td>
</tr>
<tr>
<td>Top 20 Attackers (All Attacks - last 24 hours)</td>
<td>20 IP addresses that have most frequently been the source of an attack during the last 24 hours.</td>
</tr>
<tr>
<td>Top 20 Attackers Prevented (All Attacks - last 24 hours)</td>
<td>20 IP addresses that have most frequently been prevented from attacking the network during the last 24 hours.</td>
</tr>
<tr>
<td>Top 20 Targets (last 24 hours)</td>
<td>20 IP addresses that have most frequently been the target of an attack during the last 24 hours.</td>
</tr>
<tr>
<td>Top 20 Targets Prevented (last 24 hours)</td>
<td>20 IP addresses that have most frequently prevented attacks during the last 24 hours.</td>
</tr>
<tr>
<td>All Attacks by Severity (last 24 hours)</td>
<td>Number of attacks by severity level (set in attack objects).</td>
</tr>
<tr>
<td>All Attacks Prevented by Severity (last 24 hours)</td>
<td>Number of attacks by severity level (set in attack objects).</td>
</tr>
<tr>
<td>All Attacks Over Time (last 7 days)</td>
<td>All attacks detected during the last 7 days.</td>
</tr>
<tr>
<td>All Attacks Prevented Over Time (last 7 days)</td>
<td>All attacks prevented during the last 7 days.</td>
</tr>
<tr>
<td>All Attacks Over Time (last 30 days)</td>
<td>All attacks detected during the last 30 days.</td>
</tr>
<tr>
<td>All Attacks Prevented Over Time (last 30 days)</td>
<td>All attacks prevented during the last 30 days.</td>
</tr>
<tr>
<td>Critical Attacks (last 24 hours)</td>
<td>All attacks categorized as “critical” detected during the past 24 hours.</td>
</tr>
</tbody>
</table>
Chapter 15: Reporting

Screen Reports

When the firmware on your device identifies an attack, it generates a log event. These events are totaled and summarized for your review in the reports shown in Table 90.

Table 90: Screen Reports

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical Attacks Prevented (last 24 hours)</td>
<td>All attacks categorized as “critical” prevented during the past 24 hours.</td>
</tr>
<tr>
<td>Critical Thru Medium Attacks (last 24 hours)</td>
<td>All attacks categorized as either “critical” or “medium” detected during the past 24 hours.</td>
</tr>
<tr>
<td>Critical Thru Medium Attacks Prevented (last 24 hours)</td>
<td>All attacks categorized as either “critical” or “medium” prevented during the past 24 hours.</td>
</tr>
<tr>
<td>Top 50 Scan Sources (last 7 days)</td>
<td>50 IP addresses that have most frequently performed a scan of a managed device.</td>
</tr>
<tr>
<td>Top 50 Scan Targets (last 7 days)</td>
<td>50 IP addresses that have most frequently been the target of a scan over the last 7 days.</td>
</tr>
<tr>
<td>Profiler - New Hosts (last 7 days)</td>
<td>New Hosts listed in the Profiler over the last 7 days.</td>
</tr>
<tr>
<td>Profiler - New Ports (last 7 days)</td>
<td>New Ports listed in the Profiler over the last 7 days.</td>
</tr>
<tr>
<td>Profiler - New Protocols (last 7 days)</td>
<td>New Protocols listed in the Profiler over the last 7 days.</td>
</tr>
<tr>
<td>Top IDP Rules</td>
<td>The total number of log entries generated by specific rules in your IDP policies. You can use the Top Rules report to identify those rules that are generating the most log events. This enables you to better optimize your rulebases by identifying those rules that are most and least effective. You can then modify or remove those rules from your Security Policies.</td>
</tr>
</tbody>
</table>

Screen Reports

When the firmware on your device identifies an attack, it generates a log event. These events are totaled and summarized for your review in the reports shown in Table 90.

Table 90: Screen Reports

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Screen Attacks</td>
<td>The most common attacks detected by the firmware on your security device</td>
</tr>
<tr>
<td>Screen Attacks by Severity</td>
<td>The number of attacks detected by the firmware on your security device according to severity level</td>
</tr>
<tr>
<td>Screen Attacks over Time</td>
<td>A summary of when attacks are detected by the firmware on your security device</td>
</tr>
<tr>
<td>Top Screen Attackers</td>
<td>Where attacks originate from most frequently</td>
</tr>
<tr>
<td>Top Screen Targets</td>
<td>Which hosts on your network are the most frequent targets of attackers for firewall attacks</td>
</tr>
</tbody>
</table>

Administrative Reports

Table 91 lists and describes reports in NetScreen-Security Manager that provide information specifically for administrators.
Table 91: Administrative Reports

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</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 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/DPI 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>

UAC Reports

Table 92 lists and describes those reports in NetScreen-Security Manager that provide information about Unified Access Control (UAC) session logs.

Table 92: UAC Reports

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Graph of UAC session logs</td>
<td>Total number of UAC session logs over the last 7 days.</td>
</tr>
<tr>
<td>Top 20 Destinations</td>
<td>20 destination IP addresses that have most frequently appeared on UAC logs over the last 7 days.</td>
</tr>
<tr>
<td>Top 20 Enforcers (devices) for UAC logs</td>
<td>20 Infranet enforcer devices that have most frequently appeared on UAC logs over the last 7 days.</td>
</tr>
</tbody>
</table>

For more specific information describing each report, refer to the NetScreen-Security Manager Online Help.

My Reports

Once you are comfortable using reports, you can create your own custom reports to provide the exact information that your network security needs require. My Reports are associated with a specific user across domains.

Shared Reports

You can also allow others to use your custom reports by creating them as a shared report. Shared reports are associated with domains. Subject to user-defined access control settings, shared reports are available to all other users in the domain.

Working with Reports

Using the Report Manager, you can perform the following actions:

- Generating a Predefined Report
- Creating a Custom Report
Chapter 15: Reporting

- Deleting Reports
- Organizing Reports in Folders
- Generating Reports Automatically
- Exporting Reports to HTML

Generating a Predefined Report

To generate a predefined report, click that report from the Report Manager. The report is generated according to its default report settings. You can set different report options to further tailor your reports to your specific needs. See “Setting Report Options” on page 663 for more information.

Creating a Custom Report

Both system administrators and read-only administrators can create custom reports based on their own reporting requirements.

You can also use an existing predefined report as the basis for a custom report by generating that report and saving it as custom report. You can use the same process to copy reports.

---

NOTE: All System Administrators, including those assigned a Read-Only role, can create and run their own reports.

---

Deleting Reports

If a custom report no longer serves your informational needs, you can delete it. Note however, that you cannot delete predefined reports.

To delete a custom report, select the custom report you want to delete and select Delete from the File menu. You can also right-click the report and select Delete, or use the Ctrl-D keyboard shortcut.

Organizing Reports in Folders

If you have a large number of custom reports, it is good practice to organize them in folders. You can organize your reports in folders under the My Reports and Shared Reports.

---

NOTE: You cannot create folders under any of the Predefined Reports folders.

---

To create a report folder, you need the appropriate permissions - Create Catalog Object, Delete Catalog Object and Edit Catalog Object.

After you have created a report folder, you can later edit or delete it. You cannot however, rename a folder. You can achieve the same result by saving the same report under a new folder name, and then deleting the previous folder. For more information on editing and deleting a report folder, refer to the NetScreen-Security Manager Online Help.
EXAMPLE: CREATING A CUSTOM REPORT
For example, you are a security administrator responsible for monitoring and protecting the corporate DMZ network. A Top Attacks report comes predefined in IDP, but the report displays attacks on the entire network, and you are interested only in the DMZ.

To create a custom report based on a predefined report:

1. In the Objects component, configure a network object called Corporate DMZ Network and add all the IP addresses located in the DMZ.

2. Using the Top Attacks report, use Save As to rename the report Top DMZ Attacks. You can also click the Save As... icon on the toolbar or use the Ctrl-S keyboard shortcut.


4. In the Log Filter tab, select to filter on only those destination addresses defined in the Corporate DMZ network object.

5. In the General tab, under Other Parameters use the Save Report In field to select My Reports and then edit Others to “My DMZ Reports”.

6. Click OK.

NetScreen-Security Manager creates the new report and displays it in a new folder called My DMZ Reports folder under My Reports.

NOTE: You cannot create a sub-folder under the first level of custom report folders.

Generating Reports Automatically

You can also generate reports automatically using the Scheduled Log-Based Report utility, a command line utility located on the NetScreen-Security Manager GUI Server. The utility works with scripts enabling you to generate and then send the reports to you using email or ftp.

NOTE: You cannot use the Scheduled Log-Based Report utility to generate reports defined as a My Report.

The process of creating scheduled reports involves the following 3 key steps:

- Running the report using the guiSvrCli.sh utility. This provides the login information and the report name to be created.

- Creating or editing the action script. This defines what is done with the report once run. Sample scripts are included for sending the report as e-mail and as FTP data.

- Setting a cron job to execute the guiSvrCli.sh utility with the proper parameters.
It is important to note that all of this configuration must be done from the GUI Server console, not the UI. You can verify the status of an executed report in the Job Manager.

Running Reports Using the guiSvrCLI.sh Utility

The guiSvrCLI.sh utility is located in the /usr/netscreen/GuiSvr/utils directory on the GUI Server. The syntax that affects the generation of reports is as follows:

```
export NSMUSER=global/<user name>; export NSMPASSWD=<password>; /usr/netscreen/GuiSvr/utils/guiSvrCLI.sh --generate-reports --report global:<Report Folder>\"""report name\"""" --script ftp.sh
```

The export NSMUSER and NSMPASSWORD statements set the username and password used to generate the report. This user must have appropriate rights on the NSM management system. You need to create aspecific account for this purpose.

You can generate any of the predefined reports by specifying "system" in the <Report Folder> field, or any user-created report other than those defined in "My Reports" by specifying "shared" in the <Report Folder> field. You must reference the report with the full domain path, using a colon (":" ) to separate domain elements and the report folder.

The script parameter refers to the script, located in the /usr/netscreen/GuiSvr/var/scripts directory, that is to be run on completion of the report generation.

Creating and Editing Action Scripts

Sample scripts enabling you to email and ftp the report results are available in /usr/netscreen/GuiSvr/lib/scripts for your convenience. To use these scripts, it is recommended that you first copy them to /usr/netscreen/GuiSvr/var/scripts, and then change the permissions on the scripts so that they are both writable and executable. You can then customize the scripts for your appropriate needs.

Transferring Reports to an FTP Server

One script, ftp.sh, is for transferring the report to an FTP server. The portion of the script that needs to be edited follows:

```
########################################################################
#       CONFIGURABLE PARAMETERS
########################################################################
# Remote hostname or IP address
remote_host="localhost"

# login for ftp account
userid="ftp"

# password for ftp account
passwd="ftp"

# pick reports from this directory prefix
local_dir_prefix="/usr/netscreen/GuiSvr/var"
```
Emailing Reports

To email reports, you must configure two scripts:

- `email.sh` - This is what is called in the `guiSvrCli.sh` utility and defines how the reports are to be included in the email message.
- `Email.pl` - This is what is called by the `email.sh` and configures the actual SMTP parameters.

You can attach or embed the report in the email by uncommenting a specific line in `email.sh`. You can also deliver multiple reports in separate mail messages or in a single collated one.

```
#########################################################################
#       CODE
#########################################################################

dir=`dirname $0`
cd $dir

# Each report in $1 is mailed as an attachment.
/usr/bin/perl -w email.pl -d $1 -o /dev/null

# Each report in $1 is embedded into an email and mailed.
#/usr/bin/perl -w email.pl -d $1 -embed -o /dev/null

# Each report in $1 is attached to a collated message and the collated message is mailed
#/usr/bin/perl -w email.pl -d $1 -collate -o /dev/null

# Each report in $1 is embedded into a collated message and the collated message is mailed
#/usr/bin/perl -w email.pl -d $1 -collate -embed -o /dev/null

# Don't change this line
exit $? 
```

The required SMTP settings are provided in `email.pl`.

```
#########################################################################
#       CONFIGURABLE PARAMETERS SECTION (CHANGEABLE)
#########################################################################

# From address, don't delete \ before the @ separator
my $from_addr = "user@localhost.localdomain";

# To address, don't delete \ before the @ separator
my $to_addr = "remote-user@somewhere.net";

# Email server: not required if sendmail is configured for mail transport
my $email_server = "everywhere.net";

# Subject
my $subject = "Reports are here!";

# Body text for emails with reports as attachments
my $body_text_attach = "Attached reports";

# Body text for emails with reports embedded
my $body_text_embed = "Embedded reports";
```
Using Cron with Scheduled Reports

The actual scheduling is done using the cron application. This utility executes scripts at specific times. It is configured through a file called crontab. You can edit the file using the command `crontab -e`. This invokes the vi editor and opens the crontab table.

Entries in the table consist of a command set and a schedule. The command to run the report is the same as described above.

The timing of the job is determined by a string of numbers preceding the script. There are five places and they represent, in order:

- Minute (0-59)
- Hour (0-23)
- Day of Month (1-31)
- Month (1-12)
- Day of Week (0-6) (Sunday = 0)

Use an asterisk (*) to mark a place that is not part of the given schedule. For example, to run a script every Tuesday night at 11:05 PM it would be "5 23 * * 2 Script"

EXAMPLE: USING CRON TAB TO SCHEDULE ATTACK UPDATES

In this example, if you wanted to generate a predefined report and ftp it to a server every Monday at 12:01 in the morning, you would do the following:


NOTE: The email.pl and emailReports.sh scripts only do MIME formatting of the reports. The actual mailing is done by sendmail or other Mail Transfer Agent (MTA). If you require authentication to send these reports, you must configure the authentication parameters as part of the MTA configuration. If you are using the ftp script to send you reports, you will also need to add values for the remote host, userid and password for the ftp account in the ftp.sh file.
2. Create a shell script called `reportscript.sh` with the following elements:
   - Set the NSMUSER environment variable with an NSM domain/user pair. The command for setting environment variables depends on your OS.
     
     Example: `export NSMUSER=domain/user`
   - Set the NSMPASSWD environment variable with an NSM password. The command for setting environment variables depends on your OS and shell.
     
     Example: `export NSMPASSWD=password`
   - Specify a guiSvrCli command string.
     

3. Make the script executable. Make sure the script is runnable by whoever will create the cron job.

4. Run the crontab editor.
   
   crontab -e

5. Add the following line:

   ```
   0 0 * * 1 /usr/netscreen/GuiSvr/utils/reportscript.sh
   ```

### Exporting Reports to HTML

Once you are done creating your reports, you can then export them into HTML. For example, if you wanted to share information with other security experts about the attacks that you are noticing in your network, you could use the following process to export the report onto disk:

1. Select **Export Reports** from the **File** menu. Alternatively, you could right-click in the chart window, and use the “Export reports in HTML” option. The Export Reports window appears.

2. Check the **Top Attacks** report checkbox.

3. Click **Browse** to save the file onto CD or to any other location on your desktop.

4. Click **Export**. The report is exported onto your CD.

NetScreen-Security Manager saves the report in several file formats (such as .png, .html, and .gif) that you can later display in any web browser.
Setting Report Options

Each report in NetScreen-Security Manager, by default, provides information based on data available from the current day in a horizontal bar chart. You can configure the duration, number of data points, and appearance of each report by using the Set Report Options selection in the View menu.

NOTE: You can also access the Set Report Options dialog by right-clicking the chart on each report.

Use the Set Report Options selection in the View menu to tailor your reports to display only the specific information that you want. You can configure the following options in each report:

- Report title
- Report type
- Columns for the report
- Time period
- Data point count
- Chart type

You can also access the Set Report Options dialog by right-clicking the chart on each report.

Naming a Report

You can enter a name for a new report or rename an existing report in the General tab of the Set Report Options window. You can also configure the name of the report as displayed in the report graph by editing its title.

Setting the Report Type

You can create two types of reports:

- **Time-Based**—Displays activity over time. For example, the Attacks Over Time report is a time-based report that measures the top attacks recorded in log records over a specified period.

- **Count-Based**—Displays total current activity to date. For example, the Top Scan Targets report is a count-based report that displays the total number of scans currently recorded against a specified number of destination IP addresses.

Configuring Report Source Data

You can configure a report to one of the following log record columns: Action, Alert, Src Addr, or Policy. Select the report source data by checking the appropriate checkboxes in the Columns For Report selection area. The data that you choose for the columns in your report appear in the Y-axis of the graph.
Configuring a Report Time Period

You can configure a report to display all available data from either a specific date and time or during a specific time interval.

For example, if you had reason to suspect that your network was attacked on September 15 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, then 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, then 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 50 occurrences of each data type are displayed in each report. You can configure a report to display more or fewer data points depending upon the level of detail you need. For example, if you want to obtain a more precise view of the top occurrences of events, you would configure a lower data point count (such as 25).

NOTE: The minimum data point count that you can configure in all reports is 5; the maximum data point count is 200.

Configuring the Chart Type

By default, each report depicts information in a horizontal bar chart. You can also configure the report to depict information using a pie chart.

Sharing Your Custom Report

Use the Save Report In pull-down menu and select the Shared Reports option to specify that you want to share your report across all domains.

Modifying Report Filters

You can also use report filters to reduce the amount of unwanted or unnecessary log information compiled in each report. This makes it easier for you to focus on only the log data of interest to you. You can specify criteria to filter your log data on any of the columns that you have chosen to base the report.

For example, you are a security administrator that typically reviews the “Attacks by Severity” report. You notice that critical attacks are on the rise. To track this more closely, you can modify the log filter on the “Attacks by Severity” report so that the report only displays critical attacks. To do this, you would select the “Attacks by Severity” report, and use Set Report Options to access the Log Filter tab. In the Log Filter tab, you would select to filter on attacks, and unselect all attacks except for those that are critical.
Configuring Report Processing Warnings

Each time you generate a report, it must perform a scan operation on a certain set of log records in the log database. The total number of log records that a report operation requires can have an adverse impact on your overall management performance. To prevent extraordinarily “lengthy” report operations from impacting your overall system performance, you can use the Preferences tool to configure NetScreen-Security Manager to display a warning message before a report is to scan a certain threshold number of log records.

For example, if you did not want any reports to interfere with the overall management performance, you would want to set a warning message threshold at around 1,000,000 logs. To do this you would use the Preferences option in the Tools menu and select Reports. In the New Preference Settings dialog box, click in the “Enable Warnings” checkbox and use the up and down arrows to specify 1,000,000 as the number of Maximum Records to Filter.

Once this preference is applied, a warning appears each time a report is set to perform an operation requiring 1,000,000 log records to be scanned.

Saving Your Report Settings

Once you have defined your custom reports, you can save the report settings as a custom report. Saved reports are organized under the tree node named “Custom Reports”.

Log Viewer Integration

Report Manager uses log data as the basis of all the information presented in each report. Because of this, it is recommended that you consider requirements for reporting as you decide how many log entries you want to maintain and store.

Viewing Logs From Report Manager

One key benefit of Report Manager’s tight integration with log entries is the ability to quickly access the source log data presented in each report. To view the source log entries in the Log Viewer for more detailed information about the report data, right-click a data point in any report and select Log Viewer from the View menu. The source log entries will appear in the Log Viewer.

NOTE: You cannot save the view generated in the Log Viewer for use in a later UI session.
Generating Quick Reports

Similarly, you can generate a Quick Report from data that appears in the Log Viewer or Log Investigator. Use the Quick Report tab located at the bottom of the Log Viewer or Log Investigator, and a count-based custom report called a Quick Report appears.
Figure 196: Generating Quick Reports

Top Alarms for flag

Last day as of 10/15/04 3:25:02 PM

From the Quick Report screen, you can further set report options using the pull-down menus provided to define the report. You can then save the report as a Custom Report.

Using Reports

The following examples describe typical use cases for the reports in NetScreen-Security Manager.

EXAMPLE: USING ADMINISTRATIVE REPORTS TO TRACK INCIDENTS

In this example, firewall administrators are using the Log Viewer to monitor and investigate log events. They are specifically interested in configuration changes that are causing outages sporadically throughout the network. When they encounter a configuration log that seems out of the ordinary, they are flagging the log using the predefined flag type “Investigate”.

Using Reports
After completing their investigation, they change the flag to either “Closed” or “Assigned” for further investigation. During normal operations, firewall administrators are investigating over 200 log entries per day.

You are a network manager interested in the progress of the investigation. To help track the progress, you generate a “Logs by User-set Flag” report.

By setting the duration of the report to 1 week, you can determine the total number of log entries flagged for investigation, total closed, and total assigned for further analysis.
EXAMPLE: USING ADMINISTRATIVE REPORTS TO OPTIMIZE RULEBASES

In this example, you are a security administrator responsible for implementing new rules to your firewall rulebase. After you have updated the new Security Policy on the managed security devices in your network, you are interested in knowing the effect of the new rules on network traffic.

You configure a “Top Rules” report to start at the same date and time that the new rulebase settings were updated in the network. You also set the report data point count to 100. In this way, you can get an indication for the top 100 rules that are generating log events.
By identifying the new rules that you implemented in the network, you can track how effective the new rules are. If you find that a specific rule that is permitting too much traffic, you may want to redefine it to be more strict. If you find that a specific rule is not generating any log events, you may want to check it again to verify that you configured it correctly; perhaps you configured an IP address incorrectly.

Regular review of the “Top Rules” report can help you to update and optimize the rulebases implemented in your Security Policies.

EXAMPLE: USING FW/VPN REPORT TO TRACK CONFIGURATION CHANGES
In this example, you are a firewall administrator responsible for configuring all the managed security devices in your network. You routinely update your network configurations after hours. To verify that your changes are taking effect, you routinely generate a “Top Configuration Logs” report each night at 1:00am.

During the day, you can generate a similar report to track any unauthorized configuration changes to your security devices.
Chapter 15: Reporting

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 daily generate and track an “Attacks By Severity” report.

Over time, you notice that the number of critical attacks has increased 20%. To verify this, you can also generate an “Attacks over Time” report for the past 30 days.

The report indicates a recent increase in attacks as detected by your firewall. You can generate “Top Attacks”, “Top Attackers”, and “Top Targets” reports to further investigate the nature and assess the risk of these attacks.

For details on generating and configuring these reports, refer to the NetScreen-Security Manager Online Help.

Example: Using Di Reports to Detect Application Attacks

In this example, you are a security analyst responsible for tracking potential deep inspection attacks. You routinely generate an “Attacks By Severity” report daily to track and identify potential attacks.

One day, you notice a significant increase in the number of critical attacks as detected by the deep inspection rules you have implemented in your Security Policy. You then generate a “Top Attackers” report for the last day.
The report indicates an IP address as the top attacker for all the DI attacks that you have been tracking. You recognize the IP address as an external server that is running a service using a nonstandard protocol. Although the traffic is not malicious, it happens to match a malicious signature anomaly that you have configured in your DI policy. You can then revise your policy rules to reclassify this traffic.

For details on generating and configuring these reports, refer to the NetScreen-Security Manager Online Help.

Using Statistical Reports


If you do not wish to install the NetScreen-Statistical Report Server, you can continue to use your existing Historical Report Server as part of your NetScreen-Security Manager implementation.

Refer to the NetScreen-Security Manager 2004 FP2 Migration Guide for more information about maintaining your previous implementation of Historical Report Server with NetScreen-Security Manager. You can also refer to the NetScreen-Global PRO Report Manager User’s Guide for more information about using historical reports.

Using the Watch List

NetScreen-Security Manager lets you create and configure both a destination and a source watch list. The Destination Watch List contains key hosts within the network against which a proportionally large number of logs is recorded. The Source Watch List contains key hosts outside the network that are sending a proportionally large number of log records and are therefore suspected of, or are known sources of attacks on your network.

The watch lists are convenient ways to create a list of source or destination hosts to use as a filter in:

- **Log Viewer**—Includes logs with destination or source watch lists in a query filter.

- **Log Investigator**—Investigates logs with destination or source watch lists as data point sources.

- **Report Manager**—Includes custom reports for destination and source watch lists.

Access the Destination Watch List or Source Watch List from **Tools > Preferences**. For details about creating and configuring watch lists, refer to the NetScreen-Security Manager Online Help.
The appendixes in Part 5 of the NetScreen-Security Manager Administrators Guide describe the terms used in this guide, listings of log entry categories and log entries, and other additional information you might find useful when using NetScreen-Security Manager.

Part 5 contains the following appendixes:

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

- **Appendix B, Unmanaged ScreenOS Commands** details unsupported ScreenOS CLI commands.

- **Appendix C, SurfControl Web categories** details the predefined Web categories provided and maintained by SurfControl.

- **Appendix D, Common Criteria EAL2 Compliance** describes actions required for a security administrator to properly secure the NetScreen-Security Manager system and NetScreen-Security Manager User Interface to be in compliance with the Common Criteria EAL2 security target for Juniper Networks IDP 3.0 functionality.

- **Appendix E, Log Entries** details log entry categories and subcategories.

For help in locating documentation for a term, task, or concept in this guide, see Part 6, “Index” on page 779.
Appendix A
Glossary

**Access List.** A list of network prefixes that are compared to a given route. If the route matches a network prefix defined in the access list, the route is either permitted or denied.

**Access-Challenge.** An additional condition required for a successful Telnet login by an authentication user via a RADIUS server.

**Action (Deep Inspection).** A DI action is performed by a security device when the permitted traffic matches the attack object specified in the rule. Deep Inspection actions include drop connection, drop packet, close client, and so on.

**Action (firewall).** A firewall action is performed by a security device when the device receives traffic that matches the direction, source, destination, and service. Firewall actions include permit, deny, reject.

**Activate Device Wizard.** The Activate Device wizard guides you through activating a modeled device in the NetScreen-Security Manager User Interface.

**Add Device Wizard.** The Add Device wizard guides you through importing or modeling a new device to the NetScreen-Security Manager User Interface.

**Address Object.** An address object represents a component of your network, such as a workstation, router, switch, subnetwork, or any other object that is connected to your network. Use address book objects to specify the network components you want to protect.

**Address Shifting.** A mechanism for creating a one-to-one mapping between any original address in one range of addresses and a specific translated address in a different range.

**Address Spoofing.** Address Spoofing is a technique for creating packets with a source IP address that is not the actual interface address. Attackers may use spoofed IP address to perform DDoS attacks while disguising their true address, or to take advantage of a trusted relationship between two hosts. To guard against spoofing attacks, configure a security device to check its own route table. If the IP address is not in the route table, the security device denies the traffic.

**Adjacencies.** When two routers can exchange routing information with one another, they are considered to have constructed an adjacency. Point-to-point networks have only two routers so those routers automatically form an adjacency. But point-to-multipoint networks are a series of several point-to-point networks. When routers pair in this more complex networking scheme, they are considered to be adjacent to one another.

**Advanced Encryption Standard (AES).** AES is a 128-bit encryption key standard. Use AES in your VPNs when you need greater interoperability with other network security devices.
Advertisement. A method a router uses to announce itself to other devices on the network, transmitting basic information including IP address, network mask, and other data.

Aggregate State. A router is in an aggregate state when it is one of multiple virtual BGP routing instances bundled into one address.

Aggregation. The process of combining several different routes in such a way that only a single route advertises itself. This technique minimizes the size of the routing table for the router.

Aggregator. An object used to bundle multiple routes under one common route generalized according to the value of the network mask.

Aggressive Aging. A mechanism to accelerate the timeout process when the number of sessions in the session table surpasses a specified high-watermark threshold. When the number of sessions in the table dips below a specified low-watermark threshold, the timeout process returns to normal.


APN. Access Point Name. An APN is an IE included in the header of a GTP packet that provides information on how to reach a network. It is composed of two elements: a network ID and an operator ID.

Application Layer Gateway (ALG). On a security device, an ALG is a software component that is designed to manage specific protocols such as SIP or FTP. The ALG intercepts and analyzes the specified traffic, allocates resources, and defines dynamic policies to permit the traffic to pass securely through the security device.

Area Border Router. A router with at least one interface in Area 0 and at least one interface in another area.

Area Range. A sequence of IP addresses defined by a lower limit and upper limit that indicates a series of addresses of devices that exist within an area.

Area. The most fundamental ordering method in the OSPF routing protocol. An OSPF area divides the internetwork into smaller, more manageable constituent pieces. This technique reduces the amount of information that each router must store and maintain about all the other routers. When a router in the area needs information about another device in or out of the area, it contacts a special router that stores this information. This router is called the Area Border Router (ABR) and contains all essential device information. In addition, the ABR area border router filters all information coming into the area to avoid bogging down other routers in the area with information they may not need.

AS Number. The identification number of the local autonomous system mapped to a BGP routing instance. The ID number can be any valid integer.

AS Path Access List. An access list used by a BGP routing instance to permit or deny packets sent by neighbor routing instances to the current virtual routing instance.

AS Path Attribute Class. The BGP provides four classes of path attributes. Well-Known Discretionary, Optional Transitive, and Optional Non-Transitive.

AS Path String. A string that acts as an identifier for an AS path. It is configured alongside an AS Path access list ID.

AS. See Autonomous System.
Atomic Aggregate. An object used by a BGP router to inform other BGP routers that the local system selected a generalized route.

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

Attack Objects. An attack object contains attack patterns for known attacks that attackers can use to compromise your network. Use attack objects in your firewall rules to enable your security devices to detect known attacks and prevent malicious traffic from entering your network.

Attack Protection. Attack Protection is defined by the DI Profile used in a firewall rule.

Audit Log Target. An Audit Log Target is a directive that was sent to a security device.

Audit Log Viewer. The Audit Log Viewer is a module of the NetScreen-Security Manager User Interface. The Audit Log Viewer records administrative actions. Each audit log includes the date and time the administrative action occurred, the NetScreen-Security Manager admin who performed the action, and the domain (global or a subdomain) in which the action occurred.

Authentication Header (AH). See ESP/AH.

Authentication Server Objects. An authentication server provides authentication for NetScreen-Security Manager administrators and RAS users on your network. Use authentication servers objects to set a default authentication server for the global domain and each subdomain, or access an external RADIUS or SecurID system to provide authentication.

Authentication. Authentication ensures that digital data transmissions are delivered to the intended receiver. Authentication also assures the receiver of the integrity of the message and its source (where or whom it came from). The simplest form of authentication requires a username and password to gain access to a particular account. Authentication protocols can also be based on secret-key encryption, such as DES, or on public-key systems using digital signatures.

Autonomous System (AS). An AS is a set of routers set off from the rest of the network and governed by a single technical administration. This router group uses an interior gateway protocol (IGP) or several IGPs and common metrics to route packets within the group. The group also uses an exterior gateway protocol (EGP) to route packets to other ASs. Each AS has a routing plan that indicates what destinations are reachable through it. This plan is called the Network Layer Reachability Information (NLRI) object. BGP routers generate and receive NLRI updates periodically.

Autonomous System Boundary Router. A router that connects an AS running one routing protocol to another AS running a different protocol.

Autonomous System Path. A list of all the autonomous systems that a router update has traveled through in the current transmission.

Bastion Host. A bastion host is a hardened system that is configured with the minimal software to support a single network service.

BGP Neighbor. (also known as a BGP Peer). BGP is a the Border Gateway Patrol dynamic routing protocol. A BGP neighbor is another device on the network that is running BGP.

Border Gateway Protocol (BGP). An inter-autonomous system routing protocol. BGP routers and autonomous systems exchange routing information for the Internet.
Broadcast Network. A network that connects many routers together and can send, or broadcast, a single physical message to all the attached routers. Pairs of routers on a broadcast network are assumed to be able to communicate with each other. Ethernet is an example of a broadcast network. On broadcast networks, the OSPF router dynamically detects its neighbor routers by sending Hello packets to the multicast address 224.0.0.5. For broadcast networks, the Hello protocol elects a Designated Router and Backup Designated Router for the network.

CIDR (Classless Inter-Domain Routing). An IP addressing scheme in which a single IP address is used to designate multiple unique IP addresses. A CIDR address includes an IP address and an IP network prefix.

Figure 201: CIDR Translation

<table>
<thead>
<tr>
<th>CIDR format</th>
<th>First host</th>
<th>Last host</th>
<th>Number of hosts</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.0.1/24</td>
<td>192.168.0.1</td>
<td>192.168.0.254</td>
<td>254</td>
</tr>
<tr>
<td>192.168.0.1/25</td>
<td>196.168.0.1</td>
<td>192.168.0.126</td>
<td>126</td>
</tr>
<tr>
<td>192.168.0.1/26</td>
<td>192.168.0.1</td>
<td>192.168.0.62</td>
<td>6</td>
</tr>
<tr>
<td>192.168.0.1/27</td>
<td>192.168.0.1</td>
<td>192.168.0.30</td>
<td>6</td>
</tr>
<tr>
<td>192.168.0.1/29</td>
<td>192.168.0.1</td>
<td>192.168.0.9</td>
<td>6</td>
</tr>
<tr>
<td>192.168.0.9/29</td>
<td>192.168.0.9</td>
<td>192.168.0.14</td>
<td>6</td>
</tr>
<tr>
<td>192.168.0.10/30</td>
<td>192.168.0.10</td>
<td>192.168.0.11</td>
<td>2</td>
</tr>
<tr>
<td>10.0.0.0/8</td>
<td>10.0.0.1</td>
<td>10.255.255.254</td>
<td>16777214</td>
</tr>
<tr>
<td>10.0.1.17/28</td>
<td>10.0.1.17</td>
<td>10.0.1.30</td>
<td>14</td>
</tr>
</tbody>
</table>

Circuit-level Proxy. Proxy or Proxy Server is a technique used to cache information on a Web server and acts as an intermediary between a Web client and that Web server. This proxy holds the most commonly and recently used content from the World Wide Web to provide quicker access to content for users and to increase server security.

Classless Routing. Support for interdomain routing, regardless of the size or class of the network. Network addresses are divided into three classes, but these are transparent in BGP, giving the network greater flexibility.

CLI. The CLI is the command line interface.

Cluster List. A list of paths recorded as a packet travels through a BGP route reflector cluster.

Community. A community is a grouping of BGP destination. By updating the community, you automatically update its member destinations with new attributes.

Confederation. An object inside a BGP AS that is a subset of routing instances in the AS. By grouping devices into confederations inside a BGP AS, you reduce the complexity associated with the matrix of routing connections, known as a mesh, within the AS.

Configlet. A configlet is a small, static configuration file that contains information on how a security device can connect to NetScreen-Security Manager.

CRC Errors. CRC errors indicate the number of packets generating a cyclic redundancy code error processed through the security device over the selected interface.
**Data Encryption Standard (DES).** DES is a 40- and 56-bit encryption algorithm developed by the National Institute of Standards and Technology (NIST). DES is a block encryption method originally developed by IBM. It has since been certified by the U.S. government for transmission of any data that is not classified top secret. DES uses an algorithm for private-key encryption.

**Data Encryption Standard-Cipher Block Chaining (DES-CBC).** DES-CBC is used to encrypt single DES keys.

**DCF.** See device capability file.

**Default Route.** A “catch all” routing table entry that defines the forwarding of traffic for destination networks that are not explicitly defined in the routing table. The destination network for the default route is represented by the network address 0.0.0.0/0.

**Delta.** A delta is a difference, or discrepancy. Example: the differences between the configuration running on the physical device and the difference between the configuration in NetScreen-Security Manager are known as deltas.

**De-Militarized Zone (DMZ).** A DMZ is an area between two networks that are controlled by different companies. A DMZ ethernet can be external or internal; external DMZ ethernets link regional networks with routers.

**Denial of Service (DoS) Attack.** A DoS attack is designed to disrupt a network service. Typically, an attacker sends a flood of information to overwhelm a service’s system resources, causing the server to ignore valid network requests. Other DoS attacks can cause the service process to crash.

**Device Administrator.** A device administrator is the person who uses WebUI or CLI to manage a single security device.

**Device Monitor.** The Device Monitor displays information about individual devices, their configuration and connection status, and memory usage.

**Device Server.** The Device Server is the component of the NetScreen-Security Manager management system that handles communication between the GUI Server and the device, collects data from the managed devices on your network, formats configuration information sent to your managed device, and consolidates log and event data.

**DHCP (Dynamic Host Configuration Protocol).** DHCP is used to dynamically assign IP addresses to networked computers.

**Directive.** A directive is a command send by NetScreen-Security Manager to your managed devices. Directives include importing, updating, rebooting, and so on. When you send a command to a device or group of devices, NetScreen-Security Manager creates a job for that command and displays information about that job in the Job Manager.

**Distributed Denial of Service (DDoS) Attack.** A DoS attack (typically a flood) from multiple source points. A DDoS attacks is more effective than a DoS attack, as it is no longer one computer against one server in an effort to overwhelm the server.

**DM (Data Model).** A Data Model is an XML file that contains configuration data for an individual device. The DM is stored in the Device Server; when you create, update, or import a device, the GUI Server edits the Abstract Data Model (ADM) to reflect the changes, then translates that information to the DM.

**DNS.** The Domain Name System maps domain names to IP addresses.

**Domain Menu.** The Domain Menu is the pull-down menu above the navigation tree where domains and subdomains are selected.
Domains. A domain is a logical grouping of devices, their policies, and their access privileges. A domain can contain devices, templates, objects, policies, VPNs, administrators, activities, authentication servers, groups—a representation of the all or a subset of the physical devices and functionality on your network. The domain above a domain is the parent domain, and the domain below a domain is the child domain. Domains at the same level are considered peer domains.

Dynamic Routing. A routing method which adjusts to changing network circumstances by analyzing incoming routing update messages. If the message indicates that a network change has occurred, the routing software recalculates routes and sends out new routing update messages. These messages populate the network, directing routers to rerun their algorithms and change their routing tables accordingly. There are two common forms of dynamic routing, including Distance Vector Routing and Link State Routing.

Encryption. Encryption is the process of changing data into a form that can be read only by the intended receiver. To decipher the message, the receiver of the encrypted data must have the proper decryption key. In traditional encryption schemes, the sender and the receiver use the same key to encrypt and decrypt data. Public-key encryption schemes use two keys: a public key, which anyone may use, and a corresponding private key, which is possessed only by the person who created it. With this method, anyone may send a message encrypted with the owner's public key, but only the owner has the private key necessary to decrypt it. PGP (Pretty Good Privacy) and DES (Data Encryption Standard) are two of the most popular public-key encryption schemes.

Equal Cost MultiPath. Equal Cost MultiPath (ECMP) assists with load balancing among two to four routes to the same destination or increases the effective bandwidth usage among two or more destinations. When enabled, security devices use the statically defined routes or dynamically learn multiple routes to the same destination through a routing protocol. The security device assigns routes of equal cost in round robin fashion. Default: disabled.

ESP/AH. AH and ESP are IP level security headers that were originally proposed by the Network Working Group focused on IP security mechanisms known as IPSec. The term IPSec refers to packets, keys, and routes associated with ESP and AH headers. The IP Authentication Header (AH) provides authentication. The IP Encapsulating Security Header (ESP) provides confidentiality to IP datagrams.

Ethernet. Ethernet is a local area network (LAN) technology invented at the Xerox Corporation, Palo Alto Research Center. Ethernet is a best-effort delivery system that uses CSMA/CD technology. Ethernet can be run over a variety of cable schemes, including thick coaxial, thin coaxial, twisted pair, and fiber optic cable. Ethernet is a standard for connecting computers into a local area network (LAN). The most common form of Ethernet is called 10BaseT, which denotes a peak transmission speed of 10 Mbps using copper twisted-pair cable.

Export Rules. When you have two or more virtual routers on a security device, you can configure export rules that define which routes on one virtual router are allowed to learned by another virtual router. See also Import Rules.

External Neighbors. Two BGP routers that are peers that reside in two different autonomous systems.

Extranet. An extranet connects two or more intranets. If an intranet as a company's internal Web site enables users inside the company to communicate and exchange information, an extranet connects that virtual space with another company's intranet, thus enabling these two (or more) companies to share resources and communicate over the Internet in their own virtual space. This technology greatly enhances business to business communications.

Filters. A filter organizes log entries based on admin specifications.
Firewall. A firewall device that protects and controls incoming and outgoing traffic on network connections. Firewalls protect internal servers from damage (intentional or otherwise) and enable authorized external access.

Gateway. Also called a router, a gateway is a program or a special-purpose device that transfers IP datagrams from one network to another until the final destination is reached.

GBIC. A Gigabit Interface Connector (GBIC) is the kind of interface module card used on some security devices for connecting to a fiber optic network.

GGSN. Gateway GPRS Support Node.

Gi Interface. The interface between a GSN and an external network or the Internet.

Global Domain. A domain is a logical grouping of devices, their policies, and their access privileges. The global domain is the top level, or root domain, that contains all subdomains.

GMT (Greenwich Mean Time). GMT is the Greenwich, England mean solar time. GMT is also known as Universal Time and is used for calculating time worldwide.

Gn Interface. The interface between two GSNs within the same PLMN.

Gp Interface. The interface between two GSNs located in different PLMNs.

G-PDU. A G-PDU is a user data message. It consists of a T-PDU plus a GTP header.

GPRS. General Packet Radio Service. A packet-based technology that enables high-speed wireless Internet and other data communications. GPRS provides more than three to four times greater speed than conventional GSM systems. Using a packet data service, subscribers are always connected and always online so services are easy and quick to access.

Group Expression Objects. A Group Expression Object represents a statement that sets conditions for authentication requirements, enabling you to combine multiple external user objects. You can create group expressions using the operator OR, AND, or NOT to combine user objects, user group objects, or other group expressions.

Groups. A group organizes previously-created devices into user-defined groups that make it easier for you to configure and manage devices in your domain. Groups enable you to execute certain NetScreen-Security Manager operations on multiple security devices at the same time.

GRX. GPRS Roaming Exchange.

GSM. Global System for Mobile Communications.

GTP Tunnel. A GTP tunnel in the GTP-U plane is defined for each PDP Context in the GSNs. A GTP tunnel in the GTP-C plane is defined for all PDP Contexts with the same PDP address and APN (for Tunnel Management messages) or for each MS (for messages not related to Tunnel Management). A GTP tunnel is identified in each node with a TEID, an IP address and a UDP port number. A GTP tunnel is necessary to forward packets between an external network and an MS user.

GTP. GPRS Tunneling Protocol.

GTP-C Message. GTP-Control Message. Control plane messages are exchanged between GSN pairs in a path. The control plane messages are used to transfer GSN capability information between GSN pairs, to create, update and delete GTP tunnels and for path management.

GTP-PDU. A GTP Protocol Data Unit is either a GTP-C message or a GTP-U message.
**GTP-U Message.** GTP-User Data message. User plane messages are exchanged between GSN pairs or GSN/RNC pairs in a path. The user plane messages are used to carry user data packets, and signalling messages for path management and error indication.

**GUI Server.** The GUI Server manages the system resources and data that drives NetScreen-Security Manager functionality. The GUI Server contains the NetScreen-Security Manager databases, and centralizes information for devices, their configurations, attack and server objects, and policies.

**H.323** application layer gateway (ALG) lets you to secure Voice-over-IP (VoIP) communication between terminal hosts, such as IP phones and multimedia devices. In such a telephony system, gatekeeper devices manage call registration, admission, and call status for VoIP calls. Gatekeepers can reside in the two different zones, or in the same zone.

**Hardened System.** A hardened system is a secure server with all appropriate security patches and bug fixes; these systems are designed to resist penetration.

**Hello Interval.** The amount of time that elapses between instances of Hello Packets.

**Hello Packet.** A Hello packet is a message sent out to the current network to announce the presence of the current routing instance to the network. Hello packets aid in the discovery of neighbors and in a router being able to connect to other devices on the network. When an OSPF interface is created, the interface sends Hello packets to the network to announce itself.

**Histogram.** A histogram is a vertical graph that represents different amounts by thin, color-coded bands or bars. These bars represent a frequency distribution; heights of the bars represent observed frequencies.

**HLR.** Home Location Register.

**Hold Time.** In OSPF, the maximum amount of time between instances of initiating Shortest Path First (SPF) computations. In BGP, the maximum amount of time that elapses between message transmissions between a BGP speaker and its neighbor.

**ICMP Flood.** An ICMP flood contains ICMP pings so numerous that they overload a system with echo requests, causing the system to expend all its resources responding until it can no longer process valid network traffic. If you set a threshold to invoke ICMP flood attack protection when exceeded, ICMP flood attacks are recorded as statistics.

**IE.** Information Element.

**IKE Proposal Objects.** An IKE proposal is a set of encryption keys and authentication algorithms that is used to negotiate a VPN connection. An IKE Proposal Object is a representation of an IKE proposal in the NetScreen-Security Manager UI.

**Import Rules.** When you have two or more virtual routers on a security device, you can configure import rules on one virtual router that define which routes are allowed to be learned from another virtual router. If you do not configure any import rules for a virtual router, all routes that are exported to that virtual router are accepted. See also Export Rules.

**IMSI.** International Mobile Station Identity.

**Internet Control Message Protocol (ICMP).** ICMP is a network-layer protocol that does not carry user data, but does encapsulate its messages in IP datagrams. ICMP provides a query and response system (with error-reporting) used to determine if another system on the network can receive and send data. An ICMP echo request is also known as a ping.
Internet Key Exchange (IKE). IKE is a method for exchanging keys for encryption and authentication over an unsecured medium, such as the Internet.

Internet Protocol (IP). IP is an Internet standard protocol that defines a basic unit of data called a datagram. A datagram is used in a connectionless, best-effort, delivery system. The Internet protocol defines how information gets passed between systems across the Internet.

IP Address. Each node on a TCP/IP network usually has an IP address. The IP address has a network number portion and a host number portion:

- Class A, >32,768 nodes, address format: nnn.hhh.hhh.hhh
- Class B, 256-32,768 nodes, address format: nnn.nnn.hhh.hhh
- Class C, <256 nodes, address format: nnn.nnn.nnn.hhh

This address format is called decimal dot format. The "nnn" represents a digit of a network number and "hhh" represents a digit of a host number; for example, 128.1.2.30. If you are sending data outside of your network, such as to the Internet, you need to obtain the network number from a central authority, currently the Network Information Center. See also Subnet Mask.

IP Gateway. Also called a router, an IP gateway is a program or a special-purpose device that transfers IP datagrams from one network to another until the final destination is reached.

IP Pool Objects. An IP Pool object represents a range of IP addresses. Use IP Pool object to configure a DHCP server for your managed devices.

IP Security (IPSec). IPSec is a security standard maintained by the Internet Engineering Task Force (IETF). The IPSec protocol suite provides everything you need for secure communications—authentication, integrity, and confidentiality—and makes key exchange practical even in larger networks. See also DES-CBC, ESP/AH.

IP Sweep. An IP sweep is similar to a port scan attack. Attackers perform IP sweeps by sending ICMP echo requests (or pings) to different destination addresses and wait for replies that indicate the IP address of a target. If a remote host pings 10 addresses in 0.3 seconds, the security device flags the event as an IP sweep attack and drops the connection to prevent replies.

IP Tracking. A mechanism for monitoring configured IP addresses to see if they respond to ping or ARP requests. You can configure IP tracking with NSRP to determine device or VSD group failover. You can also configure IP tracking on a device interface to determine if the interface is up or down.

ISAKMP. The Internet Security Association and Key Management Protocol (ISAKMP) provides a framework for Internet key management and provides the specific protocol support for negotiation of security attributes. By itself, it does not establish session keys, however it can be used with various session key establishment protocols to provide a complete solution to Internet key management.

Job Manager. The Job Manager is a module of the NetScreen-Security Manager User Interface. Job Manager tracks the progress of the command as it travels to the device and back to the management server.

Keepalive. The amount of time in seconds that elapses between keepalive packets which ensures that the TCP connection between the local BGP router and a neighbor router is up. This value is equal to one-third of the hold time. The default is 60 seconds.
Key Management. The only reasonable way to protect the integrity and privacy of information is to rely upon the use of secret information in the form of private keys for signing and/or encryption. The management and handling of these pieces of secret information is generally referred to as “key management.” This includes the activities of selection, exchange, storage, certification, expiration, revocation, changing, and transmission of keys. Most of the work in managing information security systems lies in the key management.

Land Attack. During a Land Attack, attackers may send spoofed SYN packets that contain the IP address of the target as both the destination and source IP address to create an empty connection. These connections flood the target system, overwhelming it and causing a denial-of-service. You can configure security devices to block Land Attack and record Land Attack attempts.

Link State Advertisement (LSA). Link State Advertisements (LSAs) are the conveyance that enables OSPF routers to make device, network, and routing information available for the link state database. Each router retrieves information from the LSAs sent by other routers on the network to construct a picture of the entire internetwork from which they distill path information to use in the routing table.

Link State. Link state routing protocols operate using an algorithm commonly called the Shortest Path First (SPF) algorithm. Instead of relying on rumored information from directly connected neighbors as in distance vector protocols, each router in a link state system maintains a complete topology of the network and computes SPF information based on the topology.

Load Balancing. Load balancing distributes workload to processors to improve the throughput of a concurrent connections.

Local Preference. To provide better information than the Multi-Exit Discriminator (MED) value provides for a packet’s path selection, BGP provides an attribute known as the LOCAL_PREF or local preference value. You can configure the LOCAL_PREF attribute so that it has a higher value for prefixes received from a router that provides a desired path to be higher than prefixes heard on the router that provides a less desirable path. The higher the value, the more preferred the route. The LOCAL_PREF attribute is the metric most often used in practice to express preferences for one set of paths over another.

Lockout. Lockout is an object state during which the object cannot be edited.

Log Category. A log category defines the log type (alarm, config, traffic, and so on.).

Log ID. A log ID is a unique ID for the log entry, derived from the combination of the date and log number.

Log Investigator. The Log Investigator is a module of the NetScreen-Security Manager User Interface. The Log Investigator contains tools for analyzing your log entries in depth. Use the Log Investigator to manipulate and change constraints on log information, correlate log entries visually and rapidly, and filter log entries while maintaining the broader picture.

Log Viewer. The Log Viewer is a module of the NetScreen-Security Manager User Interface. The Log Viewer displays log entries that your security devices generate based on criteria that you defined in your Security Policies, on the Device Server, and in the device configuration. Logs appear in table format; each row contains a single log, and each column defines specific information for a log.

Log. A Log is a grouping of log entries.

Loopback Interface. A logical interface that emulates a physical interface on the security device, but is always in the up state as long as the device is up. You must assign an IP address to a loopback interface and bind it to a security zone.

Main Display Area. The main display area displays the content for the currently selected module or module contents.
Management System. The management system includes the GUI Server and Device Server. You can deploy the GUI Server and Device Server on separate servers; however, the combination of the two servers is known as the management system.

Mapped IP Address. A MIP is a direct one-to-one mapping of traffic destined for one IP address to another IP address.

MCC. Mobile Country Code.

MD5. Message Digest (version) 5 is an algorithm that produces a 128-bit message digest (or hash) from a message of arbitrary length. The resulting hash is used to verify authenticity.

Media Gateway Control Protocol (MGCP). MGCP is a text-based, application layer protocol that can be used for call setup and call control. The protocol is based on a master/slave call control architecture: the media gateway controller (call agent) maintains call control intelligence, and media gateways carry out the instructions from the call agent.

Member AS. The name of the autonomous system being included in a BGP confederation.

Menu Bar. The menu bar is the upper section of the NetScreen-Security Manager UI. The menu bar contains accessible commands.

Metric. A value associated with a route that the virtual router uses to select the active route when there are multiple routes to the same destination network with the same preference value. The metric value for connected routes is always 0. The default metric value for static routes is 1, but you can specify a different value when defining a static route.

MNC. Mobile Network Code.

Modeling. Modeling is the process of creating a non-deployed device configuration in the NetScreen-Security Manager UI.

Modules. A module is a first-level element in the NetScreen-Security Manager navigation tree.

MS. Mobile Station.

MSIN. Mobile Subscriber Identification Number.

NAT Object. A NAT Object is a global object that contains references to device-specific NAT configurations, enabling multiple devices to share a single object. Use the Device Manager to configure NAT for each device, then create a global NAT object that includes the device-specific NAT configuration. Use global NAT objects in Security Policies and VPNs; when you update a device, that device automatically replaces the global NAT object with its device-specific NAT configuration.

NAT-Traversal (NAT-T). A method for allowing IPSec traffic to pass through NAT devices along the data path of a VPN by adding a layer of UDP encapsulation. The method first provides a means for detecting NAT devices during Phase 1 IKE exchanges, and then a means for traversing them after Phase 2 IKE negotiations are complete.

Navigation Tree. The navigation tree displays the 11 NetScreen-Security Manager modules in the left pane of the NetScreen-Security Manager window.

Neighbor. To begin configuring a BGP network, you need to establish a connection between the current device and a counterpart, adjacent device known as a neighbor or peer. While this counterpart device may seem like unneeded information at first, it is actually central to the way BGP works. Unlike RIP or OSPF, you now have to configure two devices, both the current router and its neighbor, for BGP to work. While this requires more effort, it enables networking to occur on a larger scale as BGP eludes deploying the limited advertising techniques inherent to interior networking standards.
**NetScreen Redundancy Protocol (NSRP).** NRSP is a proprietary protocol that provides configuration and run time object (RTO) redundancy and a device failover mechanism for security devices in a high availability (HA) cluster.

**NetScreen-Security Manager admin(istrator).** The NetScreen-Security Manager admin is the person who uses NetScreen-Security Manager User Interface to manage their security devices.

**Network Address Translation (NAT).** NAT is a standard for translating secure IP addresses to temporary, external, registered IP address from the address pool. NAT enables trusted networks with privately assigned IP addresses to access the Internet, eliminating the need to use a registered IP address for every machine in your network.

**NSAPI.** Network Service Access Point Identifier.

**NSGP.** NetScreen Gatekeeper Protocol.

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

**Object.** Objects represent reusable information, such as network addresses, individual users and user groups, and commonly used configuration data. In NetScreen-Security Manager, objects are shared objects, meaning they are shared between the global domain and all subdomains. Objects are the building blocks of the NetScreen-Security Manager management system.

**On-Site Admin.** The on-site admin is the person who installs a configlet using Rapid Deployment.

**Open Shortest Path First (OSPF).** A dynamic routing protocol intended to operate within a single Autonomous System.

**Packet Filtering.** Packet filtering is a router/firewall process that uses access control lists (ACL) to restrict flow of information based on protocol characteristics such as source/destination IP address, protocol, or port used. Generally, packet-filtering routers do not track sessions except when doing NAT (which tracks the session for NAT purposes).

**PDP Context.** A user session on a GPRS network.

**PDP.** Packet Data Protocol.

**PDU.** Protocol Data Unit.

**Peer.** See Neighbor

**Ping of Death.** The ping of death is an intentionally oversized or irregular ICMP packet that can trigger a Denial of Service condition, freezing, or other adverse system reactions. You can configure a security device to detect and reject oversized or irregular packet sizes.

**PLMN.** Public Land Mobile Network. A public network dedicated to the operation of mobile radio communications.

**Point-to-Multipoint Network.** A non-broadcast network where OSPF treats connections between routers as point-to-point links. There is no election of a designated router and no LSA generated for the network. A router in a point-to-multipoint network sends Hello packets to all neighbors with which it can directly communicate.
**Point-to-Point Network.** Joins two routers over a Wide Area Network (WAN). An example of a point-to-point network is two security devices connected via an IPSec VPN tunnel. On point-to-point networks, the OSPF router dynamically detects neighbor routers by sending Hello packets to the multicast address 224.0.0.5.

**Point-to-Point Protocol over Ethernet (PPPoE).** Allows multiple users at a site to share the same digital subscriber line, cable modem, or wireless connection to the Internet. You can configure PPPoE client instances, including the username and password, on any or all interfaces on some security devices.

**Policy.** A Security Policy is the combination of both firewall rulebases and all rules into a comprehensive plan that defines how the security device works on your network.

**Port Address Translation (PAT).** The translation of the original source port number in a packet to a different, randomly designated port number.

**Port Mapping.** The translation of the original destination port number in a packet to a different, predetermined port number.

**Port Mode.** A feature supported on some security devices, port mode allows you to select one of several different sets of port, interface, and zone bindings on the device. Changing the port mode removes any existing configurations on the device and requires a system reset.

**Port Scan.** A port scan attack occurs when packets are sent out to different port numbers, for the purpose of scanning the available services in hopes that one port will respond. If a remote host scans 10 ports in 0.3 seconds, the security device flags this as a port scan attack and drops the connection.

**Preference.** A value associated with a route that the virtual router uses to select the active route when there are multiple routes to the same destination network. The preference value is determined by the protocol or origin of the route. The lower the preference value of a route, the more likely the route is to be selected as the active route.

**Prefix.** An IP address that represents a route.

**Process Status.** The process status displays information about processes on a security device.

**Protocol.** Protocols are predefined services (HTTP, SNMP, Telnet, and so on) that are enabled for the security device.

**PT.** Protocol Type.

**RADIUS.** Remote Authentication Dial-In User Service is a service for authenticating and authorizing remote access service (RAS) users.

**RAS (remote access services).** RAS is the acronym for remote access services, which enable users to access services protected by your security devices. Typically, you use a VPN to enable RAS, then add RAS users to the VPN.

**Real Time Streaming Protocol (RTSP).** RTSP is an application layer protocol for controlling the delivery of a stream of real-time multimedia content.

**Realtime Monitor.** The Realtime Monitor is a module of NetScreen-Security Manager User Interface. It contains the Device Monitor, the VPN Monitor, and the NSRP Monitor.

**Receive Collisions.** The number of collisions on the line detected by the Carrier Sense Multiple Access Collision Detection (CSMA/CD) protocol.

**Redistribution List.** A list of routes the current routing domain imported from another routing domain using a different protocol.
Redistribution. The process of importing a route into the current routing domain from another part of the network that uses another routing protocol. When this occurs, the current domain has to translate all the information, particularly known routes, from the other protocol. For example, if you are on an OSPF network and it connects to a BGP network, the OSPF domain has to import all the routes from the BGP network to inform all of its devices about how to reach all the devices on the BGP network. The receipt of all the route information is known as route redistribution.

Remote Procedure Call (RPC). The RPC is a protocol that one program can use to request a service from a program located in another computer in a network.

Remote Setting Objects. A Remote Settings object defines the DNS and WINS servers that are assigned to L2TP RAS users after they have connected to the L2TP tunnel.

Report Manager. Report Manager is a module of the NetScreen-Security Manager User Interface. Use Report Manager to generate and view reports summarizing log and alarm originating from the managed security devices in your network. You can use these reports to track and analyze log incidents, network traffic and potential attacks.

Role-Based Administration (RBA). Role-based administration enables you to define strategic roles for your administrators and create domains to organize your network devices. Use role-based administration to create a security environment that reflects your current offline administrator roles and responsibilities.

Route Flap Damping. BGP provides a technique to block the advertisement of the route somewhere close to the source until the route becomes stable. This method is called flap damping. Route flap damping allows routing instability to be contained at an AS border router adjacent to the region where instability is occurring. The impact of limiting the unnecessary propagation is to maintain reasonable route change convergence time as a routing topology grows.

Route Map. Route maps are used with BGP to control and modify routing information and to define the conditions by which routes are redistributed between routing domains. A route map contains a list of route map entries, each containing a sequence number and a match and a set value. The route map entries are evaluated in the order of an incrementing sequence number. Once an entry returns a matched condition, no further route maps are evaluated. Once a match has been found, the route map carries out a permit or deny operation for the entry. If the route map entry is not a match, then the next entry is evaluated for matching criteria.

Route Redistribution. Route redistribution is the exporting of route rules from one virtual router to another.

Route Reflector. A router whose BGP configuration enables readvertising of routes between Interior BGP (IBGP) neighbors or neighbors within the same BGP AS. A route reflector client is a device that uses a route reflector to readvertise its routes to the entire AS. It also relies on that route reflector to learn about routes from the rest of the network.

Routing Information Protocol (RIP). A dynamic routing protocol used within moderate-sized autonomous systems.

Routing Table. A list in a virtual router’s memory that contains a real-time view of all the connected and remote networks to which a router is currently routing packets.

Rule. A rule is a statement that defines a specific type of network traffic. When traffic passes through the security device, the device attempts to match that traffic against its list of rules. If a rule is matched, the device performs the action defined in the rule against the matching traffic.

**Run Time Object (RTO).** A code object created dynamically in memory during normal operation. Some examples of RTOs are session table entries, ARP cache entries, certificates, DHCP leases, and IPSec Phase 2 security associations (SAs).

**Schedule Object.** A schedule object defines a time interval that a firewall rule is in effect. You use a schedule object in your firewall rule to determine when a device enforces that rule.

**Secure Copy (SCP).** A method of transferring files between a remote client and a security device using the SSH protocol. The security device acts as an SCP server, accepting connections from SCP clients on remote hosts.

**Secure Server Protocol (SSP).** For communication between the UI, the GUI Server, and the Device Server, NetScreen-Security Manager uses SSP, a modified version of TCP that is more reliable than ordinary TCP, requires less CPU and memory resources from servers, and reduces the number of acknowledgement packets on the network. SSP uses AES encryption and SH1 authentication for all connections.

**Secure Shell (SSH).** A protocol that allows device administrators to remotely manage the device in a secure manner. You can run either an SSH version 1 or version 2 server on the security device.

**Security Association.** The security association combines the Security Parameters Index and a destination address. Required for both Authentication Header and Encapsulating Security Payload protocols. See also Security Parameters Index.

**security device.** A security device enables access to your network components and protects your network against malicious traffic. NetScreen-Security Manager can manage security devices running ScreenOS 5.x and ScreenOs 4.0.x (except 4.0.2). All devices from NetScreen-5XT to the NetScreen-5400 are supported, except the NetScreen-5, NetScreen-10, and NetScreen-1000. NetScreen-Security Manager also supports the NetScreen-5GT running ScreenOS 4.0-DIAL2. NetScreen-Security Manager can also manage vsys configurations, NSRP clusters, and extranet devices.

**Security Parameters Index (SPI).** The SPI is a hexadecimal value which uniquely identifies each tunnel. It also tells the security device which key to use to decrypt packets.

**Security Policies.** A Security Policy defines access to your network, including permitted services, users, and time periods. Use Security Policies to control the shape of your network traffic as it passes through the firewall, or log specific network events.

**Security Zone.** A security zone is a collection of one or more network segments requiring the regulation of inbound and outbound traffic via access policies.

**Server Manager.** The Server Manager is a module of the NetScreen-Security Manager User Interface. Server Manager contains server objects that represent your management system components. Use Server Manager to manage and monitor the individual server processes that comprise your NetScreen-Security Manager system.

**Service Object.** Service objects represent the IP traffic types for existing protocol standards. Security devices monitor and manage network traffic using these protocols. NetScreen-Security Manager includes predefined service objects for most standard services. You can also create custom service objects to represent services that are not included in the list of predefined service objects, or to represent a custom service running on your network.
Session Description Protocol (SDP). SDP session descriptions appear in many SIP messages and provide information that a system can use to join a multimedia session. SDP might include information such as IP addresses, port numbers, times, dates, and information about the media stream.

Session Initiation Protocol (SIP). SIP is an IETF (Internet Engineering Task Force)-standard protocol for initiating, modifying, and terminating multimedia sessions over the Internet. Such sessions might include conferencing, telephony, or multimedia, with features such as instant messaging and application-level mobility in network environments.

SGSN. Serving GPRS Support Node.

SHA-1. Secure Hash Algorithm-1, an algorithm that produces a 160-bit hash from a message of arbitrary length. (It is generally regarded as more secure than MD5 because of the larger hashes it produces.)

Shared Objects. A shared object is an object that can be shared across domains.

Short Frame. A short frame contains less than 64 bytes of data.

Signalling Message. Any GTP-PDU except the G-PDU. GTP signalling messages are exchanged between GSN pairs in a path. The signalling messages are used to transfer GSN capability information between GSN pairs and to create, update and delete GTP tunnels.

Source Interface-Based Routing (SIBR). SIBR allows the security device to forward traffic based on the source interface (the interface on which the data packet arrives on the security device).

Source Route. The source route is a option in the IP header. An attacker can use the source route option to enter a network with a false IP address and have data sent back to the attacker’s real address.

Stateful Inspection. A firewall process that checks the TCP header for information on the session’s state. The process checks whether it is initializing (SYN), ongoing (SYN/ACK), or terminating (FIN). A stateful inspection firewall tracks each session flowing through it, dropping packets from unknown sessions that appear to be part of an ongoing or illegal sessions. All security devices are stateful inspectors.

Static Routing. User-defined routes that cause packets moving between a source and a destination to take a specified path. Static routing algorithms are table mappings established by the network administrator prior to the beginning of routing. These mappings do not change unless the network administrator alters them. Algorithms that use static routes are simple to design and work well in environments where network traffic is relatively predictable and where network design is relatively simple.

Status Bar. The status bar is the lower section of the NetScreen-Security Manager UI. The status bar displays supplemental information.

Subdomain. A subdomain is a domains under the global domain.

Subinterface. A subinterface is a logical division of a physical interface that borrows the bandwidth it needs from the physical interface from which it stems. A subinterface is an abstraction that functions identically to an interface for a physically present port and is distinguished by 802.1Q VLAN tagging.
**Appendix A: Glossary**

**Subnet Mask.** A subnet mask enables you to define subnetworks. For example, if you have a class B network, a subnet mask of 255.255.255.0 specifies that the first two portions of the decimal dot format are the network number, while the third portion is a subnet number. The fourth portion is the host number. If you do not want to have a subnet on a class B network, you would use a subnet mask of 255.255.0.0. A network can be subnetted into one or more physical networks which form a subset of the main network. The Subnet Mask is the part of the IP address which is used to represent a subnetwork within a network. Using Subnet Masks enables you to use network address space which is normally unavailable and ensures that network traffic does not get sent to the whole network unless intended. See also IP address.

**Super Admin(istrator).** The super administrator is the default administrator for all domains. The superadmin has immutable powers. You cannot change or delete permissions for the super administrator; you can, however, change the password for the super admin.

**SYN Attack.** A SYN attack occurs when SYN packets overwhelm a network by initiating so many connection attempts or information requests that the network can no longer process legitimate connection requests, resulting in a Denial of Service.

**Syslog.** A protocol that enables a device to send log messages to a host running the syslog daemon (syslog server). The syslog server then collects and stores these log messages locally.

**Tear Drop Attack.** A Tear Drop Attack occurs when the first and second parts of a fragmented packet overlap, the server attempting to reassemble the packet can crash. If the security device sees this discrepancy in a fragmented packet, it drops the packet.

**TEID.** Tunnel Endpoint Identifier. The TEID uniquely identifies a tunnel endpoint in the receiving GTP-U or GTP-C protocol entity. The receiving end side of a GTP tunnel locally assigns the TEID value the transmitting side has to use. The TEID values are exchanged between tunnel endpoints using GTP-C messages.

**Templates.** A template is a device configuration that you can define once and then use for multiple devices. You can specify most device configuration values in a template. In a template, you can define only those configuration parameters that you want to set; you do not need to specify a complete device configuration.

The software remembers static routes until you remove them. However, you can override static routes with dynamic routing information through judicious assignment of administrative distance values. To do this, you must ensure that the administrative distance of the static route is higher than that of the dynamic protocol.

There are two types of BGP neighbors. **internal neighbors** which are in the same autonomous system and **external neighbors** which are in different autonomous systems. A reliable connection is required between neighbors and is achieved by creating a TCP connection between the two. The handshake that occurs between the two prospect neighbors evolves through a series of phases or states before a true connection can be made. See Connection States.

**TID.** Tunnel Identifier.

**Toolbar.** The toolbar is the upper section of the NetScreen-Security Manager UI. The toolbar contains icons that relate to accessible commands.

**T-PDU.** A T-PDU is the payload that is tunnelled in the GTP tunnel.

**Transmission Control Protocol/Internet Protocol (TCP/IP).** A set of communications protocols that support peer-to-peer connectivity functions for both local and wide area networks. A communications protocol which enables computers with different operating systems to communicate with each other. Controls how data is transferred between computers on the Internet.
**Triple DES (3DES).** 3DES is a more powerful version of DES in which the original DES algorithm is applied in three rounds, using a 168-bit key. DES provides a significant performance savings but is considered unacceptable for many classified or sensitive material transfers.

**Trojan.** A trojan is a program with hidden functionality. Trojans often install a remote administration program (known as a backdoor) that enables attackers to access the target system.

**Trunk Port.** A trunk port enables a switch to bundle traffic from several VLANs through a single physical port, sorting the various packets by the VLAN identifier (VID) in their frame headers.

**Trust Zone.** One of two predefined zones that enables packets to be secured from being seen by devices external to your current domain.

**Tunnel Interface.** A tunnel 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.

**Tunneling.** A method of data encapsulation. With VPN tunneling, a mobile professional dials into a local Internet Service Provider’s Point of Presence (POP) instead of dialing directly into their corporate network. This means that no matter where mobile professionals are located, they can dial a local Internet Service Provider that supports VPN tunneling technology and gain access to their corporate network, incurring only the cost of a local telephone call. When remote users dial into their corporate network using an Internet Service Provider that supports VPN tunneling, the remote user as well as the organization knows that it is a secure connection. All remote dial-in users are authenticated by an authenticating server at the Internet Service Provider’s site and then again by another authenticating server on the corporate network. This means that only authorized remote users can access their corporate network, and can access only the hosts that they are authorized to use.

**UDP Flood.** A UDP flood is an attack using multiple UDP packets. An attacker can send UDP packets to slow the target system to the point that it can no longer handle valid connections. You can configure the security device with a threshold to invoke UDP flood attack protection; when UDP packet flow exceeds this threshold, the device records the UDP flood attack as a statistics.

**Universal Resource Locator (URL).** A URL is a standard method of specifying the location of an available electronic resource. Also known as a location or address, a URL specifies the location of files on servers. A general URL has the syntax protocol://address. For example, http://www.srl.rmit.edu.au/pd/index.html specifies that the protocol is http and the address is www.srl.rmit.edu.au/pd/index.html.

**Universal Unique IDentifier (UUID).** The UUID is a 128-bit number assigned to any object within a Distributed Computing Environment (DCE) cell which is guaranteed to be unique.

**Untrust Zone.** One of two predefined zones that enables packets to be seen by devices external to your current domain.

**User Datagram Protocol (UDP).** UDP is a protocol in the TCP/IP protocol suite that enables an application program to send datagrams to other application programs on a remote machine. UDP provides an unreliable and connectionless datagram service and does not guarantee delivery or duplicate detection; it does not use acknowledgments, or control the order of arrival.
User Interface (UI). The NetScreen-Security Manager graphical User Interface (UI) is used to control the NetScreen-Security Manager system. Using the UI, you can configure NetScreen-Security Manager administrators, add devices, edit policies, view reports, and so on.

User Object. User objects represent the users of your managed devices. You can include user objects or groups in Security Policies or VPNs to permit or deny access to individuals or groups.

User. A user is a person using the network your security devices are protecting. NetScreen-Security Manager supports two types of users: local users and external users.

View. A view is an admin-defined subset of column settings and filters in the Log Viewer.

Virtual IP Address. A VIP address maps traffic received at one IP address to another address based on the destination port number in the packet header.

Virtual Link. A logical path from a remote OSPF area to the backbone area.

Virtual Local Area Network (VLAN). A VLAN is a logical rather than physical grouping of devices that constitute a single broadcast domain. VLAN members are not identified by their location on a physical subnetwork but through the use of tags in the frame headers of their transmitted data. VLANs are described in the IEEE 802.1Q standard.

Virtual Private Network (VPN). A VPN is an easy, cost-effective and secure way for corporations to provide telecommuters and mobile professionals local dial-up access to their corporate network or to another Internet Service Provider (ISP). Secure private connections over the Internet are more cost-effective than dedicated private lines. VPNs are possible because of technologies and standards such as tunneling, screening, encryption, and IPsec.

Virtual Router (VR). A virtual router is the component of ScreenOS that performs routing functions. By default, a security device contains two virtual routers: Untrust-VR and Trust-VR.

Virtual security device (VSD). A VSD is a single logical device composed by a set of physical security devices.

Virtual Security Interface (VSI). A VSI is a logical entity at layer 3 that is linked to multiple layer 2 physical interfaces in a VSD group. The VSI binds to the physical interface of the device acting as master of the VSD group. The VSI shifts to the physical interface of another device in the VSD group if there is a failover and it becomes the new master.

Virtual System (VSYS). A virtual system is a subdivision of the main system that appears to the user to be a stand-alone entity. Virtual Systems reside separately from each other. Each one can be managed by its own Virtual System Administrator.

VPN Manager. VPN Manager is a module of the NetScreen-Security Manager User Interface. Use VPN Manager to design a system level VPN and automatically set up all connections, tunnels, and rules for all devices in the VPN.

WebTrends. A product offered by NetIQ that allows you to create customized reports based on the logs generated by a security device. When you use WebTrends, you can display the information you need in a graphical format.

Windows Internet Naming Service (WINS). WINS is a service for mapping IP addresses to NetBIOS computer names on Windows NT server-based networks. A WINS server maps a NetBIOS name used in a Windows network environment to an IP address used on an IP-based network.
**WinNuke Attack.** A WinNuke attack can crash any computer on the Internet running Windows by introducing a NetBIOS anomaly that forces Windows to restart. You can configure the security device to scan any incoming Microsoft NetBIOS Session Service packets, modify them, and record the event as a WinNuke attack.

**Worm.** A worm is a self-replicating attack program. Worms differ from typical viruses in that they are completely automatic—no attacker interaction is required. When the worm locates a vulnerable target, it immediately and automatically infects the new host with its malicious code. The newly infected host repeats the process and attempts to infect more hosts.

**XAuth.** A protocol composed of two components—remote VPN user authentication (username plus password) and TCP/IP address assignments (IP address, netmask, DNS server, and WINS server assignments).

**Zone.** A zone can be a segment of network space to which security measures are applied (a security zone), a logical segment to which a VPN tunnel interface is bound (a tunnel zone), or either a physical or a logical entity that performs a specific function (a function zone).
Appendix B
Unmanaged ScreenOS Commands

Juniper Networks NetScreen-Security Manager is designed for system-level management, enabling multiple administrators to manage their devices from one central location using the majority of CLI commands available in ScreenOS. However, a small number of device commands are unmanaged from the Juniper Networks NetScreen-Security Manager UI.

Most unmanaged commands are useful only when performing device administration on a specific device, and do not affect management capabilities (although future versions of NetScreen-Security Manager may support these commands). To use an unmanaged device command, you must connect locally to the Juniper Networks security device.

The table below details each unmanaged command.

Table 93: Unmanaged Commands for Firewall/VPN Devices

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>common-criteria</td>
<td>This command disable all internal commands. Only the root admin can set this command. If someone other than the root admin tries to set this command, the security device displays an error message.</td>
</tr>
<tr>
<td>envar</td>
<td>These commands define environment variables. Security devices use environment variables to make special configurations at startup.</td>
</tr>
<tr>
<td>gate</td>
<td>This command checks the number of gates on a security device, how many are in use, and how many are still available. Gates are logical access points in the firewall for FTP and similar applications. Security devices create the gates, then convert a gate for each new session when data traffic occurs.</td>
</tr>
<tr>
<td>ike</td>
<td>These commands define the Phase 1 and Phase 2 proposals and the gateway for an AutoKey IKE (Internet Key Exchange) VPN tunnel, and specify other IKE parameters.</td>
</tr>
<tr>
<td>intervlan-traffic</td>
<td>These commands configure inter-VLAN traffic through a security device. It is possible to configure a virtual system (vsys) with two trusted interfaces, such that traffic can enter the vsys through one interface and exit through the other without undergoing any security services such as authentication or encryption. This is known as inter-VLAN traffic.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>set interface &lt;name&gt; dhcp client settings lease &lt;minute&gt;</td>
<td>This command configures settings for DHCP client lease time.</td>
</tr>
<tr>
<td>set log audit-loss-mitigation</td>
<td>This command configures logging to mitigate message loss due to memory limitations on a security device. Used for common criteria only.</td>
</tr>
<tr>
<td>set mac</td>
<td>This command configures a static Media Access Control (MAC) address for a security device interface.</td>
</tr>
<tr>
<td>timer</td>
<td>These commands display timer settings, or configure a security device to automatically execute management or diagnosis at a specified time. All timer settings remain in the configuration script after the specified time has expired.</td>
</tr>
<tr>
<td>user</td>
<td>These commands create, remove, or display entries in the internal user authentication database.</td>
</tr>
<tr>
<td>vr nsrp-config-sync</td>
<td>This command unsets synchronization for a specific virtual router in an NSRP cluster.</td>
</tr>
</tbody>
</table>
Appendix C

SurfControl Web categories

SurfControl servers maintain a database of millions of sites organized into about 40 categories. This Appendix contains a list of the categories maintained by SurfControl and a description of the URLs in each category.

Table 94: SurfControl Web categories

<table>
<thead>
<tr>
<th>Category</th>
<th>Description of URLs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adult/Sexually Explicit</td>
<td>■ Adult products including sex toys, CD-ROMs, and videos</td>
</tr>
<tr>
<td></td>
<td>■ Adult services including video conferencing, escort services, and strip clubs</td>
</tr>
<tr>
<td></td>
<td>■ Erotic stories and textual descriptions of sexual acts</td>
</tr>
<tr>
<td></td>
<td>■ Explicit cartoons and animation</td>
</tr>
<tr>
<td></td>
<td>■ Online groups, including newsgroups and forums, that are sexually explicit in nature</td>
</tr>
<tr>
<td></td>
<td>■ Sexually-oriented or erotic full or partial nudity</td>
</tr>
<tr>
<td></td>
<td>■ Depictions or images of sexual acts, including animals or inanimate objects used in a sexual manner</td>
</tr>
<tr>
<td></td>
<td>■ Sexually exploitative or sexually violent text or graphics</td>
</tr>
<tr>
<td></td>
<td>■ Bondage, fetishes, genital piercing</td>
</tr>
<tr>
<td></td>
<td>■ Nudist sites that feature nudity</td>
</tr>
<tr>
<td></td>
<td>■ Erotic or fetish photography, which depicts nudity</td>
</tr>
</tbody>
</table>

**NOTE:** We do not include sites regarding sexual health, breast cancer, or sexually transmitted diseases (except in graphic examples).

<table>
<thead>
<tr>
<th>Advertisements</th>
<th>■ Banner Ad Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arts and Entertainment</td>
<td>■ Television, movies, music and video programming guides</td>
</tr>
<tr>
<td></td>
<td>■ Downloadable (non-streaming) movie, video or sound clips</td>
</tr>
<tr>
<td></td>
<td>■ Discussion forums on television, movies, music and videos</td>
</tr>
<tr>
<td></td>
<td>■ Online magazines and reviews on the entertainment industry</td>
</tr>
<tr>
<td></td>
<td>■ Celebrity fan sites</td>
</tr>
<tr>
<td></td>
<td>■ Horoscopes</td>
</tr>
<tr>
<td></td>
<td>■ Online greeting cards</td>
</tr>
<tr>
<td></td>
<td>■ Jokes, comics, comic books, comedians or any site designed to be funny or satirical</td>
</tr>
<tr>
<td></td>
<td>■ Circuses, theatre, variety magazines, and radio</td>
</tr>
<tr>
<td></td>
<td>■ Broadcasting firms and technologies (satellite, cable)</td>
</tr>
<tr>
<td></td>
<td>■ Book reviews and promotions, publishing houses, and poetry</td>
</tr>
<tr>
<td></td>
<td>■ Museums, galleries, artist sites (included sculpture, photography)</td>
</tr>
<tr>
<td>Category</td>
<td>Description of URLs</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Chat</td>
<td>- Web-based chat</td>
</tr>
</tbody>
</table>
| Computing and Internet   | - Reviews, information, buyer’s guides of computers, computer parts and accessories, and software  
- Computer/software/Internet companies, industry news and magazines  
- Personal storage or backup  
- Pay-to-Surf sites  
- Freeware, shareware, and software downloads  
- Clipart, fonts and animated gif pages  
- Downloadable mobile phone/ PDA games, themes, graphics, and ringtones  
- Online photo albums/ digital photo exchange                                                                                                                                                                                                 |
| Criminal Skills          | - Advocating, instructing, or giving advice on performing illegal acts such as phone, service theft, evading law enforcement, lock-picking, fraud, and burglary techniques  
- Plagiarism/cheating, including the sale of research papers                                                                                                                                                                                                                                |
| Drugs, Alcohol and Tobacco | - Recipes, instructions or kits for manufacturing or growing illicit substances, including alcohol, for purposes other than industrial usage  
- Glamorizing, encouraging, or instructing on the use of or masking the use of alcohol, tobacco, illegal drugs, or other substances that are illegal to minors  
- Alcohol and tobacco promotional Web sites  
- Information on "legal highs": glue sniffing, misuse of prescription drugs or abuse of other legal substances  
- Distributing alcohol, illegal drugs, or tobacco free or for a charge  
- Displaying, selling, or detailing use of drug paraphernalia  

**NOTE:** We do not include sites that discuss medicinal drug use, industrial hemp use, or public debate on the issue of legalizing certain drugs. Nor do we include sites sponsored by a public or private agency that provides educational information on drug use. |
| Education                | - Educational institutions, including pre-, elementary, secondary, and high schools; universities.  
- Educational sites: pre-, elementary, secondary, and high schools; universities.  
- Distance education and trade schools, including online courses.  
- Online teacher resources (lesson plans)                                                                                                                                                                                                                                              |
| Finance and Investment   | - Stock quotes, stock tickers, and fund rates  
- Online stock or equity trading  
- Online banking and bill-pay services  
- Investing advice or contacts for trading securities  
- Money management/investment services or firm  
- General finances and companies that advise thereof  
- Accountancy, actuaries, banks, mortgages, and general insurance companies                                                                                                                                                                                                 |
| Food and Drink           | - Recipes, cooking instruction and tips, food products, and wine advisors  
- Restaurants, cafes, eateries, pubs, and bars  
- Food/drink magazines, reviews                                                                                                                                                                                                                                                                 |
| Gambling                 | - Online gambling or lottery web sites that invite the use of real or virtual money  
- Information or advice for placing wagers, participating in lotteries, gambling, or running numbers  
- Virtual casinos and offshore gambling ventures  
- Virtual sports leagues and sports picks and betting pools  

**NOTE:** Casino/Hotel/Resort sites that do not feature online gambling or provide gaming tips are categorized under Travel.                                                                                                                                                                                                 |


<table>
<thead>
<tr>
<th>Category</th>
<th>Description of URLs</th>
</tr>
</thead>
</table>
| Games                         | ■ Game playing or downloading; game hosting or contest hosting  
|                               | ■ Tips and advice on games or obtaining cheat codes (“cheatz”)  
|                               | ■ Journals and magazines dedicated to game playing  
| Glamour and Intimate Apparel  | ■ Lingerie, negligee or swimwear modeling  
|                               | ■ Model fan pages; fitness models/sports celebrities  
|                               | ■ Fashion or glamour magazines online  
|                               | ■ Beauty and cosmetics  
|                               | ■ Modeling information and agencies  
| Government and Politics       | ■ Government services such as taxation, armed forces, customs bureaus, emergency services.  
|                               | ■ Local government sites  
|                               | ■ Political debate, canvassing, election information and results  
|                               | ■ Local, national, and international political sites  
| Hacking                       | ■ Promotion, instruction, or advice on the questionable or illegal use of equipment and/or software for purpose of hacking passwords, creating viruses, gaining access to other computers and/or computerized communication systems.  
|                               | ■ Sites that carry malicious executables or viruses  
|                               | ■ Sites that provide instruction or work-arounds for our filtering software  
|                               | ■ Cracked software and information sites  
|                               | ■ Pirated software and multimedia download sites  
|                               | ■ Sites that provide or promote parasites, including Spyware, Adware and other unsolicited commercial software  
| Hate                          | ■ Advocating or inciting degradation or attack of specified populations or institutions based on associations such as religion, race, nationality, gender, age, disability, or sexual orientation  
|                               | ■ Promoting a political or social agenda that is supremacist in nature and exclusionary of others based on their race, religion, nationality, gender, age, disability, or sexual orientation  
|                               | ■ Holocaust revisionist/denial sites  
|                               | ■ Coercion or recruitment for membership in a gang* or cult**  
|                               | ■ Militancy, extremist  
|                               | ■ Flagrantly insensitive or offensive material  

**NOTE:** We do not include news, historical, or press incidents that may include the above criteria (except in graphic examples).

**A gang is defined as:** a group whose primary activities are the commission of felonious criminal acts, which has a common name or identifying sign or symbol, and whose members individually or collectively engage in criminal activity in the name of the group.

**A cult is defined as:** a group whose followers have been deceptively and manipulatively recruited and retained through undue influence such that followers’ personalities and behavior are altered. Leadership is all-powerful, ideology is totalistic, and the will of the individual is subordinate to the group. Sets itself outside of society.
<table>
<thead>
<tr>
<th>Category</th>
<th>Description of URLs</th>
</tr>
</thead>
</table>
| Health and Medicine   | - General health such as fitness and well-being  
- Medical information about ailments, conditions, and drugs  
- Medical reference  
- Medical procedures, including elective and cosmetic surgery  
- Alternative and complementary therapies  
- Prescription medicines  
- Hospital, medical insurance  
- Dentistry, optometry, and other medical-related sites  
- General psychiatry and mental well-being sites  
- Promoting self-healing of physical and mental abuses, ailments, and addictions  
- Psychology, self-help books, and organizations |
| Hobbies and Recreation| - Recreational pastimes such as collecting, gardening, kit airplanes  
- Outdoor recreational activities such as hiking, camping, rock climbing  
- Tips or trends focused on a specific art, craft, or technique  
- Online publications on a specific pastime or recreational activity  
- Online clubs, associations or forums dedicated to a hobby  
- Traditional (board, card) games and their enthusiasts  
- Animal/pet related sites, including breed-specific sites, training, shows and humane societies |
| Hosting Sites          | - Web sites that host business and individuals' web pages (such as GeoCities, earthlink.net, AOL)                                                                 |
| Job Search and Career Development | - Employment agencies, contractors, job listings, career information  
- Career searches, career-networking groups |
| Kid's Sites            | - Child oriented sites and sites published by children                                                                                                                                                 |
| Lifestyle and Culture  | - Homelife and family-related topics, including parenting tips, gay/lesbian/bisexual (non-pornographic sites), weddings, births, and funerals  
- Foreign cultures, socio-cultural information |
| Motor Vehicles         | - Car reviews, vehicle purchasing or sales tips, parts catalogs  
- Auto trading, photos, discussion of vehicles including motorcycles, boats, cars, trucks and RVs  
- Journals and magazines on vehicle modification, repair, and customizing  
- Online automotive enthusiast clubs |
| News                   | - Newspapers online  
- Headline news sites, newswire services, and personalized news services  
- Weather sites |
| Personals and Dating   | - Singles listings, matchmaking and dating services  
- Advice for dating or relationships; romance tips and suggestions |
| Photo Searches         | - Sites that provide resources for photo and image searches |
| Real Estate            | - Home, apartment, and land listings  
- Rental or relocation services  
- Tips on buying or selling a home  
- Real estate agents  
- Home improvement and inspection sites |
<table>
<thead>
<tr>
<th>Category</th>
<th>Description of URLs</th>
</tr>
</thead>
</table>
| Reference         | - Personal, professional, or educational reference  
                            - Online dictionaries, maps, and language translation sites  
                            - Census, almanacs, and library catalogues  
                            - Topic-specific search engines                                                                                                                         |
| Religion          | - Churches, synagogues, and other houses of worship  
                            - Any faith or religious beliefs, including non-traditional religions such as Wicca and witchcraft                                               |
| Remote Proxies    | - Remote proxies or anonymous surfing  
                            - Web-based translation sites that circumvent filtering  
                            - Peer-to-peer sharing                                                                                                                                      |
| Sex Education     | - Pictures or text advocating the proper use of contraceptives  
                            - Sites relating to discussion about the use of the Pill, IUDs and other types of contraceptives  
                            - Discussion sites on how to talk to your partner about diseases, pregnancy and respecting boundaries  
                            
                            **NOTE:** Not included in the category are commercial sites that sell sexual paraphernalia. These sites are typically found in the Adult category. |
| Search Engines    | - General search engines (Yahoo, AltaVista, Google)                                                                                                      |
| Shopping          | - Online auctions  
                            - Department stores, retail stores, company catalogs and other sites that allow online consumer shopping  
                            - Online downloadable product warehouses; specialty items for sale  
                            - Freebies or merchandise giveaways                                                                                                                       |
| Sports            | - Team or conference web sites  
                            - National, international, college, professional scores and schedules  
                            - Sports-related online magazines or newsletters                                                                                                         |
| Streaming Media   | - Streaming media files or events (any live or archived audio or video file)  
                            - Internet TV and radio  
                            - Personal (non-explicit) webcam sites  
                            - Telephony sites that allow users to make calls via the Internet                                                                                       |
| Travel            | - Airlines and flight booking agencies  
                            - Accommodation information  
                            - Travel package listings  
                            - City guides and tourist information  
                            - Weather bureaus  
                            - Car Rentals                                                                                                                                             |
| Usenet News/Forums| - Newsgroups  
                            - Opinion or discussion forums  
                            - Weblog (blog) sites                                                                                                                                 |
| Usenet News/Forums| - Newsgroups  
                            - Opinion or discussion forums  
                            - Weblog (blog) sites                                                                                                                                 |
<table>
<thead>
<tr>
<th>Category</th>
<th>Description of URLs</th>
</tr>
</thead>
</table>
| Violence/Offensive   | ■ Portraying, describing or advocating physical assault against humans, animals, or institutions  
■ Depictions of torture, mutilation, gore, or horrific death  
■ Advocating, encouraging, or depicting self-endangerment, or suicide, including through eating disorders or addictions  
■ Instructions, recipes or kits for making bombs or other harmful or destructive devices  
■ Excessive use of profanity or obscene gesticulation  
■ Sites promoting terrorism  
■ Excessively violent sports or games  
■ Offensive or violent language or satire  
**NOTE:** We do not block news, historical, or press incidents that may include the above criteria (except in graphic examples). |
| Weapons              | ■ Online purchasing or ordering information, including lists of prices and dealer locations  
■ Any page or site predominantly containing, or providing links to, content related to the sale of guns, weapons, ammunition or poisonous substances  
■ Displaying or detailing the use of guns, weapons, ammunition or poisonous substances  
■ Clubs which offer training on machine guns, automatics and other assault weapons and/or sniper training  
**NOTE:** Weapons are defined as something (as a club, knife, or gun) used to injure, defeat, or destroy. |
| Web-based E-mail     | ■ Web-based e-mail accounts  
■ Messaging sites                                                                                           |
Appendix D
Common Criteria EAL2 Compliance

This appendix describes actions required for a security administrator to properly secure the NetScreen-Security Manager system and NetScreen-Security Manager User Interface to be in compliance with the Common Criteria EAL2 security target for Juniper Networks IDP 4.0 functionality.

The NetScreen-Security Manager system consists of the Device Server and the Gui Server; the NetScreen-Security Manager User Interface is a client application used to access information stored in the NetScreen-Security Manager system.

Guidance for Intended Usage
- The NetScreen-Security Manager system must be installed on dedicated systems. These dedicated systems must not contain user processes that are not required to operate the NetScreen-Security Manager software.

Guidance for Personnel
- There must be one or more competent individuals assigned to manage the NetScreen-Security Manager system and User Interface (UI), and the security of the information that they contain.
- The authorized administrators must not be careless, willfully negligent, or hostile and must follow and abide by the instructions provided by the NetScreen-Security Manager documentation.
- The NetScreen-Security Manager system and UI must be accessed only by authorized users.

Guidance for Physical Protection
- The processing resources of the NetScreen-Security Manager system and UI must be located within facilities with controlled access that prevents unauthorized physical access.
Appendix E
Log Entries

This appendix lists the log entry subcategories for the following log entry categories:

- Screen Alarm Log Entries
- Alarm Log Entries
- Deep Inspection Alarm Log Entries
- Configuration Log Entries
- Information Log Entries
- Self Log Entries
- Traffic Log Entries

Additionally, you can also view the information provided for Basic and Extended GTP Log Entries.
### Screen Alarm Log Entries

The Screen category contains the following subcategories:

Table 95: Screen Alarm Log Entries

<table>
<thead>
<tr>
<th>Attack</th>
<th>ScreenOS Message ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address Sweep Attack</td>
<td>Attacks &gt; Alert &gt; 00017</td>
</tr>
<tr>
<td>Block ActiveX component</td>
<td>Attacks &gt; Critical &gt; 00434</td>
</tr>
<tr>
<td>Block EXE component</td>
<td>Attacks &gt; Critical &gt; 00433</td>
</tr>
<tr>
<td>Block IP fragment traffic</td>
<td>Attacks &gt; Critical &gt; 00429</td>
</tr>
<tr>
<td>Block JAVA component</td>
<td>Attacks &gt; Critical &gt; 00432</td>
</tr>
<tr>
<td>Block ZIP component</td>
<td>Attacks &gt; Critical &gt; 00431</td>
</tr>
<tr>
<td>Destination IP session limit</td>
<td>Attacks &gt; Critical &gt; 00430</td>
</tr>
<tr>
<td>ICMP Flood Attack</td>
<td>Attacks &gt; Alert &gt; 00011</td>
</tr>
<tr>
<td>IDS ICMP Fragment</td>
<td>Attacks &gt; Critical &gt; 00422</td>
</tr>
<tr>
<td>IDS ICMP too large</td>
<td>Attacks &gt; Critical &gt; 00436</td>
</tr>
<tr>
<td>IDS IP Bad Options</td>
<td>Attacks &gt; Critical &gt; 00415</td>
</tr>
<tr>
<td>IDS IP unknown port</td>
<td>Attacks &gt; Critical &gt; 00414</td>
</tr>
<tr>
<td>IDS SYN Fragment</td>
<td>Attacks &gt; Critical &gt; 00412</td>
</tr>
<tr>
<td>IDS TCP FIN No ACK</td>
<td>Attacks &gt; Critical &gt; 00438</td>
</tr>
<tr>
<td>IDS TCP SYN FIN</td>
<td>Attacks &gt; Critical &gt; 00437</td>
</tr>
<tr>
<td>IDS TCP No Flag</td>
<td>Attacks &gt; Critical &gt; 00413</td>
</tr>
<tr>
<td>IP Source Route Attack</td>
<td>Attacks &gt; Alert &gt; 00009</td>
</tr>
<tr>
<td>IP Spoof Attack</td>
<td>Attacks &gt; Alert &gt; 00008</td>
</tr>
<tr>
<td>Land Attack</td>
<td>Attacks &gt; Alert &gt; 00010</td>
</tr>
<tr>
<td>Malicious URL Protection</td>
<td>Attacks &gt; Critical &gt; 00032</td>
</tr>
<tr>
<td>Multiple Authentications Failed</td>
<td>Auth &gt; Alert &gt; 00003</td>
</tr>
<tr>
<td>Ping of Death Attack</td>
<td>Attacks &gt; Emergency &gt; 00007</td>
</tr>
<tr>
<td>Policy Denied</td>
<td>Policies &gt; Alert &gt; 00018</td>
</tr>
<tr>
<td>Port Scan Attack</td>
<td>Attacks &gt; Alert &gt; 00016</td>
</tr>
<tr>
<td>SYN Attack</td>
<td>Attacks &gt; Emergency &gt; 00005</td>
</tr>
<tr>
<td>SYN Flood</td>
<td></td>
</tr>
<tr>
<td>SYN ACK</td>
<td></td>
</tr>
<tr>
<td>SYN MAC</td>
<td></td>
</tr>
<tr>
<td>SYN-ACK-ACK proxy DoS</td>
<td>Attacks &gt; Critical &gt; 00439</td>
</tr>
<tr>
<td>Source IP session limit</td>
<td>Attacks &gt; Critical &gt; 00033</td>
</tr>
<tr>
<td>Tear Drop Attack</td>
<td>Attacks &gt; Emergency &gt; 00006</td>
</tr>
<tr>
<td>UDP Flood Attack</td>
<td>Attacks &gt; Alert &gt; 00012</td>
</tr>
<tr>
<td>VPN Replay Detected</td>
<td>IKE &gt; Critical &gt; 00042</td>
</tr>
<tr>
<td>Winnuke Attack</td>
<td>Attack &gt; Alert &gt; 00004</td>
</tr>
</tbody>
</table>
The Alarm category contains the following subcategories:

Table 96: Alarm Log Entries

<table>
<thead>
<tr>
<th>Alarm Log Entry Subcategories</th>
<th>ScreenOS Message ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin</td>
<td>Admin &gt; Alert &gt; 00027</td>
</tr>
<tr>
<td>Anti Virus - CSP</td>
<td>AntiVirus Scanning (External) &gt; Error &gt; 0052</td>
</tr>
<tr>
<td>BGP Alarm</td>
<td>BGP &gt; Alert &gt; 00206</td>
</tr>
<tr>
<td>CPU Usage High</td>
<td>Logging &gt; Critical &gt; 00030</td>
</tr>
<tr>
<td>DHCP</td>
<td>DHCP &gt; Alert &gt; 00029</td>
</tr>
<tr>
<td></td>
<td>DHCP &gt; Critical &gt; 00029</td>
</tr>
<tr>
<td>DNS Host</td>
<td>DNS &gt; Critical &gt; 00021</td>
</tr>
<tr>
<td>Interface Failover</td>
<td>Interface &gt; Critical &gt; 00090</td>
</tr>
<tr>
<td>Hardware</td>
<td>Device &gt; Critical &gt; 00022</td>
</tr>
<tr>
<td>IP Conflict</td>
<td>ARP &gt; Critical &gt; 00031</td>
</tr>
<tr>
<td>Log Overflow</td>
<td>Logging &gt; Critical &gt; 00024</td>
</tr>
<tr>
<td>Memory Low</td>
<td>Device &gt; Critical &gt; 00020</td>
</tr>
<tr>
<td></td>
<td>Logging &gt; Critical &gt; 00020</td>
</tr>
<tr>
<td>NSRP Inconsistent Config</td>
<td>High Availability &gt; 00015</td>
</tr>
<tr>
<td>NSRP IP DUP Master</td>
<td>High Availability &gt; 00015</td>
</tr>
<tr>
<td>NSRP RTO DOWN</td>
<td>High Availability &gt; 00015</td>
</tr>
<tr>
<td>NSRP RTO Duplicate</td>
<td>High Availability &gt; 00015</td>
</tr>
<tr>
<td>NSRP RTO UP</td>
<td>High Availability &gt; 00015</td>
</tr>
<tr>
<td>NSRP Status</td>
<td>High Availability &gt; Critical &gt; 00015</td>
</tr>
<tr>
<td>NSRP TRACKIP Failed</td>
<td>High Availability &gt; 00062</td>
</tr>
<tr>
<td>NSRP TRACKIP Failover</td>
<td>High Availability &gt; 00062</td>
</tr>
<tr>
<td>NSRP VSD 2nd Path Reply</td>
<td>High Availability &gt; Critical &gt; 00077</td>
</tr>
<tr>
<td>NSRP VSD 2nd Path REQ</td>
<td>High Availability &gt; Critical &gt; 00076</td>
</tr>
<tr>
<td>NSRP VSD Backup</td>
<td>High Availability &gt; Critical &gt; 00073</td>
</tr>
<tr>
<td>NSRP VSD Ineligible</td>
<td>High Availability &gt; Critical &gt; 00074</td>
</tr>
<tr>
<td>NSRP VSD Init</td>
<td>High Availability &gt; Critical &gt; 00070</td>
</tr>
<tr>
<td>NSRP VSD Inoperable</td>
<td>High Availability &gt; Critical &gt; 00075</td>
</tr>
<tr>
<td>NSRP VSD Master</td>
<td>High Availability &gt; Critical &gt; 00071</td>
</tr>
<tr>
<td>NSRP VSD Pbackup</td>
<td>High Availability &gt; Critical &gt; 00072</td>
</tr>
<tr>
<td>OSPF Packet Flood</td>
<td>OSPF &gt; Critical &gt; 00206</td>
</tr>
<tr>
<td>RIP Packet Flood</td>
<td>RIP &gt; Critical &gt; 207</td>
</tr>
<tr>
<td>Route add/delete Error</td>
<td>OSPF &gt; Critical &gt; 200</td>
</tr>
<tr>
<td>Route RIP Updated Flood</td>
<td>RIP &gt; Critical &gt; 00207</td>
</tr>
<tr>
<td>Exceeded Route Entry (Sys)</td>
<td>Route &gt; Critical &gt; 00200</td>
</tr>
<tr>
<td>Secure Shell</td>
<td>SSH &gt; Critical &gt; 00034</td>
</tr>
</tbody>
</table>
## Deep Inspection Alarm Log Entries

The Deep Inspection Alarm category contains the following subcategories:

<table>
<thead>
<tr>
<th>Attack Name</th>
<th>Attack Description</th>
<th>Severity</th>
<th>Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>APP:CURL-OF-BANNER</td>
<td>This signature detects buffer overflow attempts against the cURL file retrieval client. cURL 6.1 to 7.4 versions are vulnerable. Attackers may use a malicious server to connect to the cURL client and execute arbitrary code with the permissions of the cURL user.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>CHAT:AIM:MESSAGE-SEND</td>
<td>This signature detects messages sent from AIM clients to other AIM clients.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>CHAT:AUDIT:AIM:INVALID-TLV</td>
<td>This protocol anomaly is a AIM message with an invalid TLV; the TLV data specified in the FLAP header is less than the actual data in the TLV header.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>CHAT:AUDIT:AIM:INV-TLV-LEN</td>
<td>This protocol anomaly is a AIM message with an invalid TLV; the TLV length is less than expected, or the TLV length is greater than the data specified in the FLAP header.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>CHAT:AUDIT:MSN:GROUP-NAME</td>
<td>This protocol anomaly is an MSN message with a group name length that exceeds the user-defined maximum. The default group name maximum is 64.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>CHAT:AUDIT:YMSG:FILE-SEND</td>
<td>This signature detects a Yahoo Messenger client sending a file to another user.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>CHAT:AUDIT:YMSG:MAIL-ADDR</td>
<td>This protocol anomaly is a Yahoo! Messenger email address that exceeds the user-defined maximum. A Yahoo! Messenger server sends an email address as part of a new email alert message. The default number of bytes in an Yahoo! Messenger email address is 84.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>CHAT:AUDIT:YMSG:MSG-TOO-BIG</td>
<td>This protocol anomaly is a Yahoo! Messenger message that exceeds the user-defined maximum. The default number of bytes in an Yahoo! Messenger message is 8192.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>CHAT:AUDIT:YMSG:OFLOW-GRP-NAME</td>
<td>This protocol anomaly is a Yahoo! Messenger group name that exceeds the user-defined maximum. Yahoo! Messenger clients use groups to separate their friends into categories. The default number of bytes in an Yahoo! Messenger group name is 84.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>CHAT:AUDIT:YMSG:OFLOW-PASSWD</td>
<td>This protocol anomaly is a Yahoo! Messenger encrypted password that exceeds the user-defined maximum. The Yahoo! Messenger client sends an encrypted password to the server as part of the authentication process. The default number of bytes in an Yahoo! Messenger encrypted password is 1024.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
</tbody>
</table>
### Appendix E: Log Entries

<table>
<thead>
<tr>
<th>Attack Name</th>
<th>Attack Description</th>
<th>Severity</th>
<th>Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHAT:MSN:ACCESS</td>
<td>This signature detects MSN Messenger chat using the specified content type &quot;text/plain&quot; on port 1863 (default port of MSN Messenger).</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>CHAT:MSN:LOGIN-ATTEMPT</td>
<td>This signature detects attempts to login to the MSN network using an MSN Messenger client.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>DB:MS-SQL:SQLXML-ISAPI-OF</td>
<td>This signature detects buffer overflow attempts against the SQLXML-ASAPI Extension in Microsoft SQL Server 2000. The SQLXML-ASAPI extension handles data queries over HTTP (SQLXML HTTP); attackers may connect to the target host and submit maliciously crafted data to create a buffer overflow.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>DNS:AUDIT:CLASS-NON-IN</td>
<td>This protocol anomaly is a DNS request/reply in which the question/resource address class is not IN (Internet Address). Although allowed by the RFC, this should happen only in rare circumstances and may indicate an exploit attempt.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>DNS:AUDIT:QCLASS-UNEXP</td>
<td>This protocol anomaly is a DNS reply with a resource specifying a CLASS ID reserved for queries only (QCLASS). This may indicate an exploit attempt.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>DNS:AUDIT:REP-QTYPE-UNEXPECTED</td>
<td>This protocol anomaly is a DNS reply with a resource specifying a TYPE ID reserved for queries only (QTYPE). This may indicate an exploit attempt.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>DNS:AUDIT:REP-S2C-QUERY</td>
<td>This protocol anomaly is a DNS reply with a query/reply bit (QR) that is unset (indicating a query). This may indicate an exploit attempt.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>DNS:AUDIT:REQ-C2S-RESPONSE</td>
<td>This protocol anomaly is a DNS request with a query/reply bit (QR) set (indicating a reply). This may indicate an exploit attempt.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>DNS:AUDIT:REQ-INVALID-HDR-RA</td>
<td>This protocol anomaly is a client-to-server DNS message with the recursion-available bit (RA) set. This may indicate an exploit attempt.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>DNS:AUDIT:TYPE-ANY</td>
<td>This protocol anomaly is a DNS request with request type set to &quot;ANY&quot;.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>DNS:EXPLOIT:EMPTY-UDP-MSG</td>
<td>This protocol anomaly is an empty DNS UDP message. This may indicate an exploit attempt.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>DNS:EXPLOIT:EXPLOIT-BIND9-RT</td>
<td>This protocol anomaly is an rdataset parameter to the dns_message_findtype() function in message.c that is not NULL. In BIND 9 (up to 9.2.0), attackers may cause a shutdown on an assertion failure. Note: Common queries in routine operations (such as SMTP queries) may trigger this anomaly.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>DNS:EXPLOIT:POINTER-LOOP</td>
<td>This protocol anomaly is a DNS message with a set of DNS pointers that form a loop. This may indicate a denial-of-service (DoS) attempt.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>DNS:EXPLOIT:REQUEST-SHORT-MSG</td>
<td>This protocol anomaly is a DNS message that ended prematurely. This may indicate an exploit attempt.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>DNS:EXPLOIT:TYPE-AXFR</td>
<td>This protocol anomaly is a zone transfer attempt. This may indicate an attempt to obtain information about an entire domain.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>DNS:HEADERERROR:INVALID-OPC</td>
<td>This protocol anomaly is a DNS request/reply with an invalid value in the header OPCODE field. This may indicate an exploit attempt.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------</td>
<td>-------------------</td>
</tr>
<tr>
<td>DNS:OVERFLOW:FF-FF-BIN</td>
<td>This signature detects attempts to create buffer overflows. Attackers may send maliciously crafted packets to DNS servers to overflow the buffer and gain root access.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>DNS:OVERFLOW:INVALID-LABEL-LEN</td>
<td>This protocol anomaly is a DNS request/reply with a label that exceeds the maximum length (63) specified in the RFC. This may indicate a buffer overflow attempt.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>DNS:OVERFLOW:INVALID-POINTER</td>
<td>This protocol anomaly is a DNS request/reply with a pointer that points beyond the end of the data. This may indicate a buffer overflow or denial-of-service (DoS) attempt.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>DNS:OVERFLOW:NAME-TOO-LONG</td>
<td>This protocol anomaly is a DNS name that exceeds 255 characters. This may cause problems for some DNS servers.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>DNS:OVERFLOW:NXT-OVERFLOW</td>
<td>This protocol anomaly is a suspiciously large NXT resource record in a DNS transaction. BIND versions 8.2 through 8.2.1 are vulnerable to a buffer overflow in the processing of NXT resource records.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>DNS:OVERFLOW:OPT-DOS</td>
<td>This protocol anomaly is a suspiciously long OPT resource record. All versions of BIND up to version 8.3.3 are vulnerable to a denial of service attack. An attacker can crash the server by requesting a subdomain that does not exist with an OPT resource record that has a very large UDP payload size.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>DNS:OVERFLOW:OVERSIZED-UDP-MSG</td>
<td>This protocol anomaly is a DNS UDP-based request/reply that exceeds the maximum length (512) specified in RFC. This may indicate a buffer overflow attempt.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>DNS:OVERFLOW:SIG-OVERFLOW</td>
<td>This protocol anomaly is a TCP-based DNS transaction with a suspiciously small SIG resource record. Bind versions 8 to 8.3.3 are vulnerable to a heap overflow in the code that handles SIG resource records. Attackers may execute arbitrary code on the server.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>DNS:OVERFLOW:TOO-LONG-TCP-MSG</td>
<td>This protocol anomaly is a DNS TCP-based request/reply that exceeds the maximum length specified in the message header. This may indicate a buffer overflow or an exploit attempt.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>DNS:QUERY:NULL-QUERY</td>
<td>This protocol anomaly is a DNS request with the question, answer, additional, and name server counts are zero. This can indicate a malicious user trying to crash the DNS server.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>DNS:QUERY:VERSION-QUERY</td>
<td>This protocol anomaly is a DNS query for version.bind with the type set to TXT and the class set to CHAOS. BIND servers support the ability to be remotely queried for their versions. This can indicate a reconnaissance attempt; when attackers know the BIND version, they can then attempt to exploit vulnerabilities on the server.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>DOS:NETDEV:CISCO-HTTPD-DOS</td>
<td>This signature detects attempts to exploit a vulnerability in Cisco IOS. Versions prior to 11.0, 11.2.8SA1, 12.1(1a)T1, and 12.1(1.3)T are susceptible. Attackers may remotely request URLs containing the %% string from the IP HTTP server, causing the router to crash/reboot/power cycle.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>DOS:NETDEV:CISCO-RTR-DOS</td>
<td>This signature detects denial-of-service (DoS) attempts against Cisco (routers). Cisco has identified multiple affected versions of IOS and customers are advised to check with their vendor or on Cisco's Web site for information. Attackers may send invalid HTTP traffic to a Cisco IOS device to cause a DoS on the device.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-------------</td>
<td>--------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>DOS:NETDEV:LINKSYS-GOZILA-DOS2</td>
<td>This signature detects attempts to exploit a vulnerability in a LinkSys Cable/DSL router. Attackers may submit an overly long sysPasswd parameter within a malicious HTTP request to crash a LinkSys Cable/DSL router.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>DOS:NETDEV:LINKSYS-GOZILA-DOS3</td>
<td>This signature detects attempts to exploit a vulnerability in a LinkSys Cable/DSL router. Attackers may submit an overly long DomainName parameter within a malicious HTTP request to crash a LinkSys Cable/DSL router.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>DOS:NETDEV:NETWORK-3COM-DOS</td>
<td>This signature detects attempts to exploit a firmware vulnerability in the 3COM OfficeConnect 812 and 840 DSL/ADSL routers. OCR812 versions 1.1.9 and earlier are susceptible. Attackers may remotely request long strings from the HTTP daemon, making the router reboot/power cycle and creating a denial-of-service (DoS).</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>DOS:NETDEV:WEBJET-FRAMEWORK</td>
<td>This signature detects attempts to exploit a vulnerability in HP Web JetAdmin service. Web JetAdmin version 6.5 is vulnerable. Attackers may access sensitive configuration information. If you run an HP Web JetAdmin server on your network, configure DI to monitor the server port that is configured to listen; by default, the listening port is TCP/8000.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>DOS:NETDEV:WEBJET-FW-INFOLEAK</td>
<td>This signature detects attempts to exploit a vulnerability in HP Web JetAdmin service. Web JetAdmin version 6.5 is vulnerable. Attackers may access sensitive configuration information.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>DOS:NETDEV:WEBJET-TRAVERSAL</td>
<td>This signature detects directory traversal attempts against HP Web JetAdmin service. HP Web JetAdmin version 7.5.2546 and earlier are vulnerable. Because JetAdmin does not properly verify input to the setinclude parameter in /plugins/hpjdwm/script/test/setinfo.hts, attackers may use a directory traversal to read and execute arbitrary HTS files.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>DOS:NETDEV:WEBJET-WRITETOFILE</td>
<td>This signature detects attempts to exploit a vulnerability in HP Web JetAdmin service. Web JetAdmin versions 7.x are vulnerable. Attackers may send a maliciously formatted request to a Web JetAdmin script to execute arbitrary commands on the server.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>FTP:COMMAND:PLATFTP-CD-DOS</td>
<td>This signature detects attempts to exploit a vulnerability in PlatinumFTP. Attackers may submit a maliciously crafted pathname in a CD request to crash the FTP daemon. PlatinumFTP 1.0.6 and earlier versions are vulnerable.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:COMMAND:SITE-EXEC</td>
<td>This signature detects attempts to exploit a configuration vulnerability in wuFTPd. Version 2.4.1 is susceptible. pathnames.h sets __PATH_EXECPATH to /bin, which is relative to ~ ftp for anonymous users, but relative to / for users with accounts (specifying the actual /bin rather than ~ ftp/bin). Attackers may establish an FTP account on the system and run the site exec command to gain access to the /bin directory.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:DIRECTORY:DOT-DOT</td>
<td>This signature detects '../..' FTP commands sent to FTP/21. Attackers may change the directory to the root directory of the FTP service, and gain access to the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-------------</td>
<td>--------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>FTP:DIRECTORY:MSIE-FTP-DIRTRA/</td>
<td>This signature detects a Microsoft Internet Explorer client attempting to download a file from a malicious server. The server may embed a directory traversal attack in the filename to specify the exact file download location on the client machine.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>FTP:EXPLOIT:BOUNCE-ATTACK</td>
<td>This protocol anomaly is an FTP bounce attack. There are two possibilities: a PORT command specified an IP address different from the client address, or a PASV command resulted in a 227 message with an IP address different than the server.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:EXPLOIT:FTPBIN-WRITEABLE</td>
<td>This signature detects an attempt by a malicious attacker to upload files with the names of common binaries to the FTP server's /bin directory. Successful exploitation of this vulnerability may result in the attacker being able to execute arbitrary code on the victim ftp server, including the reading of sensitive files outside of the ftp server's path.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>FTP:EXPLOIT:ILLEGAL-PORT</td>
<td>This protocol anomaly is an FTP PORT command/response to a PASV command (&quot;227...&quot;) that specifies a reserved port number. This may indicate a attempts to make the firewall open reserved ports.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:EXPLOIT:OPENFTPD-MSG-FS</td>
<td>This signature detects attempts to exploit a format string vulnerability in the OpenFTP daemon.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>FTP:EXPLOIT:SYNTAX-ERROR</td>
<td>This protocol anomaly is a syntax error in an FTP command/response, such as a malformed PORT command or 227 response. This may indicate an exploit attempt.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:EXPLOIT:TYPOFT-DOS</td>
<td>This signature detects denial-of-service (DoS) attempts against TypSoft FTP Server. TypSoft FTP Server 1.10 and earlier versions are vulnerable. Attackers may send known malicious FTP path strings to exhaust all system resources and crash a TypSoft FTP Server.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:EXPLOIT:WIN32-WFTPD-BOF</td>
<td>This signature detects invalid LIST, NLST, and STAT commands. WS-FTPD for Windows (trial versions 3.20 and 3.21, Pro and Standard) contains a vulnerability in the command parser that may allow malicious users to crash the service or execute arbitrary code. WS-FTPD for Windows (trial versions 3.20 and 3.21, Pro and Standard) contains a vulnerability in the command parser that may allow malicious users to crash the service or execute arbitrary code.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>FTP:FILE:FTP-PUT-AUTOEXECBAT</td>
<td>This signature detects an attempt by an attacker to exploit a directory traversal vulnerability in the SunFTP daemon. Successful exploitation of this vulnerability may allow an attacker to read and write to files outside of the daemon's directory structure. This vulnerability is present in SunFTP build 9.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>FTP:MS-FTP:ASTERISK</td>
<td>This signature detects denial-of-service (DoS) attempts against Microsoft FTP Service in Microsoft IIS 4.0 and 5.0. Attackers who have previously established an FTP session may send glob characters within a maliciously crafted NLST request to crash the server.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:MS-FTP:STAT-GLOB</td>
<td>This signature detects denial-of-service (DoS) attempts against Microsoft FTP Service in Microsoft IIS 4.0 and 5.0. Attackers who have previously established an FTP session may send glob characters within a maliciously crafted status request to crash the server.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>FTP:OVERFLOW:BSD-FTPD-MKD-OF</td>
<td>This signature detects buffer overflow attempts against the FTPD that ships with early versions of FreeBSD 4.x and OpenBSD 2.8. FTPD 6.00LS and 6.5/OpenBSD versions are vulnerable. Attackers may gain local host access and root permissions.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:OVERFLOW:FREEBSD-FTPD-GLOB</td>
<td>This signature detects buffer overflow attempts against the FreeBSD FTP daemon. FreeBSD-4.2 is vulnerable. Attackers may submit a malicious STAT request that contains file globbing characters to execute arbitrary code on the target host with administrator privileges.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:OVERFLOW:LINE_TOO_LONG</td>
<td>This protocol anomaly is an incoming FTP line that is too long. This may indicate an attempt to overflow the server.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:OVERFLOW:OPENBSD-X86</td>
<td>This signature detects buffer overflow attempts against ftpd in OpenBSD. OpenBSD versions 2.7 and 2.8, FTP code revisions 1.49 to 1.79 are vulnerable. Attackers with write access may exploit the replydirname() function in BSD-based ftpd daemons to gain root access.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:OVERFLOW:PASS_TOO_LONG</td>
<td>This protocol anomaly is an FTP client password that exceeds the length threshold. This may indicate a malicious FTP client attempting to overflow the server.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:OVERFLOW:PATH-LINUX-X86-1</td>
<td>This signature detects attempts to exploit a realpath vulnerability in ProFTPD and wuFTPd running on LINUX. Versions ProFTPD 1.2pre1 and earlier and wuFTPd 2.4.2 (beta 18) VR9 and earlier are susceptible. Attackers may gain write access, remotely create long pathnames, and overflow the buffer to gain root access.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:OVERFLOW:PATH-LINUX-X86-2</td>
<td>This signature detects attempts to exploit a realpath vulnerability in ProFTPD and wuFTPd running on LINUX. Versions ProFTPD 1.2pre1 and earlier and wuFTPd 2.4.2 (beta 18) VR9 and earlier are susceptible. Attackers may gain write access, remotely create long pathnames, and overflow the buffer to gain root access.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:OVERFLOW:PATH-LINUX-X86-3</td>
<td>This signature detects attempts to exploit a realpath vulnerability in ProFTPD and wuFTPd running on LINUX. Versions ProFTPD 1.2pre1 and earlier and wuFTPd 2.4.2 (beta 18) VR9 and earlier are susceptible. Attackers may gain write access, remotely create long pathnames, and overflow the buffer to gain root access.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:OVERFLOW:PATH-TOO-LONG</td>
<td>This protocol anomaly is a pathname in an FTP command (RETR, STOR, APPE, SMNT, RNFR, RNTO, DELE, RMD, MKD, STAT, CWD, LIST, NLST) that exceeds the length threshold. This may be an attempt to overflow the server.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:OVERFLOW:SITESTRING-2-LONG</td>
<td>This protocol anomaly is an argument in the FTP SITE command that exceeds the length threshold. This may be an attempt to overflow the server.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:OVERFLOW:USERNAME-2-LONG</td>
<td>This protocol anomaly is a username in an FTP connection that exceeds the length threshold. This may be an attempt to overflow the server.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:OVERFLOW:WFTPD-MKD-OVERFLOW</td>
<td>This signature detects buffer overflow attempts against the MKD command in Wftpd server 2.34. Attackers may use MKD and CWD commands to create nested directories and execute arbitrary commands with system privileges.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>--------------</td>
</tr>
<tr>
<td>FTP:OVERFLOW:WUBSD-SE-RACE</td>
<td>This signature detects buffer overflow attempts against the PASS command in Wu-ftpd 2.6.0 and BSDi-ftpd. Attackers may send a maliciously crafted PASS request to an FTP server to execute arbitrary commands as root.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:PABLO-FTP:FORMAT-STRING</td>
<td>This signature detects denial of service attempts against the Pablo FTP Server. Versions 1.2, 1.3, and 1.5 running on Windows 2000 are vulnerable. Because the FTP server improperly parses format string characters, attackers may supply a maliciously crafted username to execute arbitrary code and crash the server.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:PASSWORD:BRUTE-FORCE</td>
<td>This protocol anomaly is multiple login failures within a short period of time between a unique pair of hosts.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>FTP:PASSWORD:COMMON-PASSWD</td>
<td>This signature detects common passwords used in FTP sessions. Attackers may attempt to log into known accounts using easily guessed passwords.</td>
<td>info</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:PASSWORD:H0TB0X</td>
<td>This signature detects attempts to use the default rootkit password ‘h0tb0x’ to access a FreeBSD rootkit account. Attackers may gain root access.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:PASSWORD:LRKR0X</td>
<td>This signature detects attempts to install the Rootkit hacker utility on a LINUX system. The default password is lrkr0x.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:PASSWORD:SATORI</td>
<td>This signature detects attempts to install the Rootkit lrk4 hacker utility on a system. The default password is satori.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:PASSWORD:WH00T</td>
<td>This signature detects attempts to install the Rootkit hacker utility on a LINUX system. The default password is wh00t.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:PROFTP:LOGKFR-OF1</td>
<td>This signature detects buffer overflow attempts against the log_xfer() function in ProFTPD. This vulnerability affects ProFTPD versions 1.2.0pre1, pre2, and pre3.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:PROFTP:MKD-OVERFLOW</td>
<td>This signature detects buffer overflow attempts against ProFTPD. Versions 1.2pre3 and earlier are vulnerable. Attackers may send a pathname to the ‘MKD’ command to gain remote root access.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:PROFTP:PPC-FS1</td>
<td>This signature detects attempts to exploit a format string vulnerability in ProFTPD. Versions 1.2pre6 and earlier are vulnerable. Attackers may overflow the PWD command.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:PROFTP:PPC-FS2</td>
<td>This signature detects attempts to exploit a format string vulnerability in ProFTPD. Versions 1.2pre6 and earlier are vulnerable.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:PROFTP:PROFTPD-GEN-GLOB-DOS</td>
<td>This signature detects denial-of-service (DoS) attempts against ProFTPD. Because ProFTPD uses inadequate globbing algorithms, attackers may send wildcards in the argument of a maliciously crafted command to DoS the server.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:PROFTP:SIZE-DOS2</td>
<td>This signature detects attempts to exploit a vulnerability in ProFTPD. Version 1.2.0pre* is vulnerable. Attackers may send multiple SIZE requests with a static pathname to create a denial-of-service (DoS).</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:PROFTP:USER-DOS</td>
<td>This signature detects attempts to exploit a vulnerability in ProFTPD. Versions 1.2.0rc* and 1.2.0pre* are vulnerable. Attackers may send a maliciously crafted USER command to create a denial-of-service (DoS).</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>-----------</td>
</tr>
<tr>
<td>FTP:REQERR:GNULS-WIDTH-DOS</td>
<td>This signature detects denial-of-service (DoS) attempts against GNU ls. If the FTP daemon uses a vulnerable version of GNU ls, attackers may send an oversized width parameter to GNU ls to cause the server CPU utilization to temporarily reach 100% and exhaust system memory. This condition can persist for several minutes depending on the width specified.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:REQERR:REQ-MISSING-ARGS</td>
<td>This protocol anomaly is an FTP command with an incomplete argument list, such as a USER command with no user name, a RETR command with no file name, etc. This may indicate command line access to the FTP server or an exploit attempt.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:SERVU:CHMOD-OVERFLOW</td>
<td>This signature detects attempts to exploit a vulnerability in the ServU FTP server CHMOD command. The CHMOD command is typically used to change the permissions of a file on the server. Attackers may send an overly long filename argument to the CHMOD command to execute arbitrary code with system privileges.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>FTP:USER:ROOT</td>
<td>This signature detects attempts to login to an FTP server using the “root” account. This may indicate an attacker trying to gain root-level access, or it may indicate poor security practices. FTP typically uses plain-text passwords, and using the root account to FTP could expose sensitive data over the network.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:WS-FTP:CPWD</td>
<td>This signature detects buffer overflow attempts against WS FTP Server. The code that handles arguments to the SITE CPWD command, which allows users to change their password, contains an unchecked string copy. Attackers may send a maliciously crafted argument in the SITE CPWD command to overflow the buffer and overwrite the return address.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:WU-FTP:DELE-OF</td>
<td>This signature detects buffer overflow attempts against the DELE command in a WU-ftpd server. Wu-ftpd versions 2.4 and prior (Academ beta12-18 included) are vulnerable. This may be a variation on the ADM exploit; attackers may log in anonymously using a hardcoded email address as the password.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:WU-FTP:FTPD-BSD-X86</td>
<td>This signature detects attempts to exploit an input validation vulnerability in wuFTpd running on FreeBSD. FreeBSD versions 4.3 and 4.4 are vulnerable. Because user input goes directly into a format string for a *printf function, attackers may overwrite data on a stack (i.e. a return address), access the shellcode pointed to by the overwritten eip, and execute arbitrary commands.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:WU-FTP:GLOBARG</td>
<td>This signature detects attempts to exploit a vulnerability in Wu-ftpd, a software package that provides File Transfer Protocol (FTP) services for UNIX and Linux systems. Wu-ftpd versions 2.6.1 to 2.6.18 are vulnerable. Attackers may send a maliciously crafted pathname in a CWD or LIST command to the FTP server to execute arbitrary commands as root.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>FTP:WU-FTP:IREPLY-FS</td>
<td>This signature detects attempts to exploit a format string vulnerability in Wu-ftpd 2.4 running on Solaris 2.8. Attackers may inject malicious code into the Wu-ftpd daemon memory space; later in the same session, the attacker may exploit a format string vulnerability in the ireply() function to access that code and execute arbitrary commands as root.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:WU-FTP:LINUX-OF</td>
<td>This signature detects attempts to exploit an input validation vulnerability in wuFTPd running on LINUX. All versions are susceptible. Because user input goes directly into a format string for a *printf function, attackers may overwrite data on a stack, i.e. a return address, access the shellcode pointed to by the overwritten eip, and execute arbitrary commands. This same attack may be successful seen against ProFTPD servers.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:WU-FTP:REALPATH-OF</td>
<td>This signature detects buffer overflow attempts against the realpath() function in Wu-ftpd, a software package that provides File Transfer Protocol (FTP) services for UNIX and Linux systems. Wu-ftpd version 2.5.0 and earlier are vulnerable. Attackers may send a maliciously crafted FTP pathname to overflow a buffer in realpath() and execute arbitrary commands with administrator privileges.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>FTP:WU-FTP:REALPATH-OF2</td>
<td>This signature detects buffer overflow attempts against the realpath() function in Wu-ftpd, a software package that provides File Transfer Protocol (FTP) services for UNIX and Linux systems. Wu-ftpd version 2.5.0 and earlier are vulnerable. Attackers may send a maliciously crafted FTP pathname to overflow a buffer in realpath() and execute arbitrary commands with administrator privileges.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:3COM:3COM-PASS-LEAK</td>
<td>This signature detects attempts to access a 3COM wireless router web page that contains sensitive administrative information. No authentication is required to access this page.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:3COM:ADMIN-LOGOUT</td>
<td>This signature detects direct requests to the logout web service on a 3Com 3crwe754g72-a based device. Attackers that are spoofing a 3Com administrator's IP address may call the logout application to force the administrator to logout.</td>
<td>info</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:3COM:CONF-DOWNLOAD</td>
<td>This signature detects attempts to download the configuration file from a 3Com 3crwe754g72-a based device. Attackers may use the sensitive information obtained from the configuration file to gain full control over the device.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:3COM:LOG-CLEAN</td>
<td>This signature detects attempts to cause a 3Com 3crwe754g72-a based device to clear its logs. Attackers may use spoofed IP address to send a log clear request without authenticating.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:APACHE:APACHE-BADIPV6</td>
<td>This signature detects attempts to exploit a vulnerability in Apache Web server. All Apache servers on all platforms running version Apache 2.0.50 and earlier are vulnerable. Using apr-util, attackers may include a crafted IPv6 literal address within an HTTP request to an Apache v2 server to cause the Apache child process to quit. On BSD systems, attackers may also be able to execute arbitrary code.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>HTTP:APACHE:APACHE-BADIPV6-2</td>
<td>This signature detects attempts to exploit a vulnerability in Apache Web server. All Apache servers on all platforms running version Apache 2.0.50 and earlier are vulnerable. Using apr-util, attackers may include a crafted IPv6 literal address within an HTTP request to an Apache v2 server to cause the Apache child process to quit. On BSD systems, attackers may also be able to execute arbitrary code.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:APACHE:CHUNKED-WORM</td>
<td>This signature detects attempts to infect Apache Web servers with the Apache Worm. Apache versions 1.3.26, 2.0.38 and prior are vulnerable. Apache improperly calculates required buffer sizes for chunked encoded requests due to a signed interpretation of an unsigned integer value. The worm sends POST requests containing malicious chunked encoded data to exploit the Apache daemon.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:APACHE:MOD-NTLM-BOF1</td>
<td>This signature detects buffer overflow attempts against Apache Web server. An Apache Web server uses mod_ntlm (an Apache 1.x and 2.x module) to authenticate users against a Microsoft Windows Domain Controller. Attackers may send long or malformed strings to mod_ntlm using the Authorization HTTP header, overflow the buffer, then execute arbitrary code on the Web server.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:APACHE:MODPHP-UPLOAD-HOF</td>
<td>This signature detects heap overflow attempts against mod_php in Apache. Attackers may send a maliciously crafted HTTP POST request to execute arbitrary code on the server.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:APACHE:NOSEJOB</td>
<td>This signature detects attempts to exploit a vulnerability in Apache Web servers. Apache improperly calculates required buffer sizes for chunked encoded requests due to a signed interpretation of an unsigned integer value. Attackers may send chunked encoded requests with the unique Host header value “Apache-nosejob.c.” in the GET request to create a buffer overflow and execute arbitrary code.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:APACHE:PHP-INVALID-HDR</td>
<td>This signature detects denial-of-service attempts against the Apache HTTP daemon. PHP versions 4.2.0 and 4.2.1 running on Apache 1.3.26 are vulnerable. Attackers may use invalid headers in an HTTP request to crash the Apache HTTP daemon; the daemon may require a manual restart.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:APACHE:REDHAT-DIRLIST</td>
<td>By submitting a malformed HTTP GET request to an Apache server using the default configuration supplied with several versions of RedHat Linux an attacker can cause the web server to return a listing of the contents of that directory, even if an index page is present.</td>
<td>low</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:APACHE:RESIN-WEB-INF</td>
<td>This signature detects attempts to exploit a flaw in Resin 2.1.12, a Java Scriptlet server. Attackers can send malformed URL requests to a server to allow access to a normally protected sub-directory, the WEB-INF directory.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:APACHE:SCALP</td>
<td>This signature detects attempts to exploit a vulnerability in Apache Web servers. Apache improperly calculates required buffer sizes for chunked encoded requests due to a signed interpretation of an unsigned integer value. Attackers may send chunked encoded requests with the unique Host header value “apache-scalp.c.” in the GET request to create a buffer overflow and execute arbitrary code.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>--------------</td>
</tr>
<tr>
<td>HTTP:AUDIT:MSNG-HTTP-VER</td>
<td>This protocol anomaly is an HTTP request with no version number after the 'HTTP/...'. This may indicate command line access to an HTTP server.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:AUDIT:UNKOWN-REQ</td>
<td>This protocol anomaly is an unknown HTTP request. Known requests are OPTION, GET, HEAD, POST, PUT, DELETE, TRACE, and CONNECT.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:BADBLUE:INVALID-GET-DOS</td>
<td>This signature detects denial-of-service attempts against Working Resources BadBlue Web server. Attackers may send a maliciously crafted HTTP GET request to the Web server to disable the daemon and render it unusable until restarted.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:BADBLUE:PROXY-RELAY</td>
<td>This signature detects attempts to relay a web request through a BadBlue web server. When BadBlue is using its default configuration, attackers may use the web server as a proxy server to attack internal targets or mask attack activity.</td>
<td>medium</td>
<td>sos5.1.0, sos5.0.0</td>
</tr>
<tr>
<td>HTTP:BIGBROTHER:DIR-TRAVERSAL</td>
<td>This signature detects attempts to view files on the Web server using the BigBrother bb-hist.sh history browser script. Attackers may view any files on the Web server that are accessible to the user the history browser script is running under.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:CGI:ALTAVISTA-TRAVERSAL</td>
<td>This signature detects attempts to exploit a vulnerability in the AltaVista Search engine. The search engine sets up a Web server at port 9000 that listens for search queries. The search function accepts a single '../' string in the query, providing access to the parent, or 'http' directory. This directory typically contains administrative documents that may include the password for the remote administration utility, which is base-64 encoded. Attackers may send multiple '../' strings in hex code (ie.'%2e%2e%2f') in a query to access the remote administration utility password and gain full remote administration abilities.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:CGI:ANYFORM-SEMICOLON</td>
<td>This signature detects attempts to exploit the AnyForm CGI script, a popular CGI form designed to support simple forms that deliver responses via email. Some versions of AnyForm did not perform user supplied data sanity checking, and may allow remote execution of arbitrary commands on the server.</td>
<td>high</td>
<td>sos5.1.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:CGI:APPLE-QT-FILEDISC1</td>
<td>This signature detects attempts to exploit a vulnerability in Apple QuickTimer Streaming Server. QuickTime Streaming Server v4.1.1 and earlier versions are vulnerable. Attackers may send a maliciously crafted URL to parse_xml.cgi to view files that are not usually accessible through HTTP.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:CGI:AXIS-ACCOUNT</td>
<td>This signature detects a request to an Axis Video Server containing parameters designed to create an Administrator account on the server.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:CGI:BNB-SURVEY-REMOTE-EXEC</td>
<td>This signature detects attempts to access the BNBSurvey survey.cgi program. Attackers may remotely execute commands via shell metacharacters.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:CGI:BUGZILLA-SEMICOLON</td>
<td>This signature detects shell access attempts to exploit the process_bug.cgi script vulnerability in Bugzilla. Attackers may send a semi-colon as an argument to the script, followed by arbitrary shell commands.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>------------</td>
</tr>
<tr>
<td>HTTP:CGI:DCFORUM-AZ-EXEC</td>
<td>This signature detects shell attempts to exploit the dcforum.cgi script in DCScripts DC Forum (all versions), which is used to manage web-based discussion boards. Attackers may use maliciously crafted URL requests with the pipe and newline characters to execute arbitrary scripts on the Web server.</td>
<td>medium</td>
<td>sos5.0.0,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:CGI:FORMMAIL-ENV-VAR</td>
<td>This signature detects access to the FormMail CGI program. Attackers may use this program to remotely execute commands.</td>
<td>medium</td>
<td>sos5.0.0,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:CGI:HASAN-DIR-TRAVERSAL</td>
<td>This signature detects attempts to exploit a vulnerability in the Hassan shopping cart script shop.cgi. Attackers may access arbitrary system files.</td>
<td>medium</td>
<td>sos5.0.0,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:CGI:HTDIG-INCLUSION</td>
<td>This signature detects attempts to exploit a vulnerability in the /dig, a Web content search engine for UNIX. Because /dig improperly validates form input, attackers may pass a maliciously crafted variable to the htssearch CGI script to read files accessible to the program user.</td>
<td>medium</td>
<td>sos5.0.0,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:CGI:HYPERSEEK-DIR-TRAVERSAL</td>
<td>This signature detects attempts to exploit a vulnerability in the hsx.cgi, which ships as part of iWeb Hyperseek 2000. Attackers may view arbitrary files and directories.</td>
<td>medium</td>
<td>sos5.0.0,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:CGI:IKONBOARD-BADCOOKIE</td>
<td>This signature detects attempts to exploit a vulnerability in IkonBoard, a popular Web-based discussion board. Attackers may send a maliciously crafted cookie that contains illegal characters to IkonBoard to execute arbitrary code with IkonBoard privileges (typically user level).</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:CGI:INFO2WWW-EXEC</td>
<td>This signature detects attempts to exploit a vulnerability in the info2www CGI script. Attackers may execute arbitrary binaries on the Web server.</td>
<td>medium</td>
<td>sos5.0.0,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:CGI:INFOSRCH-REMOTE-EXEC</td>
<td>This signature detects attempts to exploit a vulnerability in the infosrch.cgi script. Attackers may execute commands on the Web server.</td>
<td>medium</td>
<td>sos5.0.0,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:CGI:LIBCGI-RFP-OVERWRITE</td>
<td>This signature detects attempts to exploit a vulnerability in the LIB CGI. Attackers may inject maliciously crafted C code into LIB CGI applications to overwrite the Frame Pointer and execute arbitrary code on the host.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:CGI:MOREOVER-CACHE-FEED</td>
<td>This signature detects attempts to exploit a vulnerability in the cached_feed.cgi script provided by moreover.com. Attackers may view arbitrary system files that are readable by the HTTPd process.</td>
<td>medium</td>
<td>sos5.0.0,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:CGI:TECHNOTE-MAIN-DCLSR</td>
<td>This signature detects directory traversal attempts that exploit the main.cgi script in TECH-NOTE 2000. Because the script validates input incorrectly, attackers may remotely access arbitrary files from the server.</td>
<td>medium</td>
<td>sos5.0.0,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:CGI:TECHNOTE-PRINT-DCLSR</td>
<td>This signature detects directory traversal attempts that exploit the print.cgi script in TECH-NOTE 2000. Because the script validates input incorrectly, attackers may remotely access arbitrary files from the server.</td>
<td>medium</td>
<td>sos5.0.0,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:CGI:W3-MSQL-CGI-OF</td>
<td>This signature detects attempts to exploit a vulnerability in W3-ssql, a CGI program that acts as a Web interface for Mini SQL (mSQL). W3-ssql version 2.0.11 is vulnerable. Attackers may remotely send a maliciously crafted scanf call to overflow the content-length field and execute arbitrary code with Web server privileges.</td>
<td>medium</td>
<td>sos5.0.0,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>------------</td>
</tr>
<tr>
<td>HTTP:CGI:W3-MSQL-FILE-DISCLSR</td>
<td>This signature detects buffer overflow attempts that exploit the w3-msql CGI script in mini-SQL. Attackers may execute arbitrary commands on the server.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:CGI:WEBPALS-EXEC</td>
<td>This signature detects attempts to exploit a vulnerability in the WebPALS CGI script. Attackers may remotely execute arbitrary code with root permissions.</td>
<td>critical</td>
<td>sos5.0.0,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:CGI:WEBSPEED-WSADMIN</td>
<td>This signature detects attempts to gain administrative access to the WebSpeed server without normal authentication.</td>
<td>critical</td>
<td>sos5.0.0,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:CGI:WEBSPIRS-FILE-DISCLSR</td>
<td>This signature detects attempts to exploit a vulnerability in the SilverPlatter WebSPIRS webspirs.cgi file. Attackers may access arbitrary system files</td>
<td>medium</td>
<td>sos5.0.0,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:CGI:YABB-DIR-TRAVERSAL</td>
<td>This signature detects attempts to exploit a vulnerability in the YaBB.pl CGI script. Attackers may view arbitrary files.</td>
<td>medium</td>
<td>sos5.0.0,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:CHKP:AUTH-FMT-STR</td>
<td>This signature detects attempts to exploit a vulnerability in some Web servers and Web proxies. Attackers may send user authentication that includes format strings to crash some Web servers, creating a denial-of-service (DoS) or enabling the attackers to take control of the firewall as root.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:CHKP:FW1-FORMAT-STR</td>
<td>This signature detects attempts to exploit a vulnerability in the CheckPoint AI/Smart Defense HTTP proxy engine. Attackers may send a scheme that includes format strings to crash the proxy engine, creating a denial-of-service (DoS) or enabling the attackers to take control of the firewall as root.</td>
<td>critical</td>
<td>sos5.0.0,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:CHKP:FW1-PROXY</td>
<td>This signature detects attempts to exploit the web proxy functions of CheckPoint FireWall-1. When the HTTP CONNECT method, used to build generic Transit Layer Security over HTTP, is used by default, the firewall web proxies may be used as open TCP proxies. Attackers may use an HTTP proxy to connect to a server, then use the CONNECT method to access other servers and launch further attacks.</td>
<td>medium</td>
<td>sos5.0.0,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:CISCO:IOS-ADMIN-ACCESS</td>
<td>This signature detects attempts to exploit a vulnerability in Cisco IOS. Attackers may remotely gain full administrative access to the router.</td>
<td>critical</td>
<td>sos5.0.0,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:CISCO:VOIP:PORT-INFO-DOS</td>
<td>This signature detects attempts to exploit a vulnerability in Cisco VoIP phones. Versions CP-7910 and later are vulnerable. Attackers may send an arbitrarily long (120000+) StreamID to the PortInformation script to cause an error message that displays a memory dump. Attackers may use this information to reconstruct the calling patterns of a particular phone.</td>
<td>medium</td>
<td>sos5.0.0,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:CISCO:VOIP:STREAM-ID-DOS</td>
<td>This signature detects denial-of-service (DoS) attempts against Cisco VoIP phones. Versions CP-7910 and later are vulnerable. Attackers may send an arbitrarily long (120000+) StreamID to the StreamingStatistics script to cause the phone to reset, creating a DoS for 30 seconds (or until the phone reboots).</td>
<td>medium</td>
<td>sos5.0.0,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:COLDFUSION:EXPRCALC-OPNFL</td>
<td>This signature detects attempts to exploit a vulnerability in the ColdFusion ExprCalc.cfm script. Attackers may delete files from a Web server.</td>
<td>medium</td>
<td>sos5.0.0,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>HTTP:COLDFUSION:HEADER-LOG-OF</td>
<td>This signature detects attempts to exploit a vulnerability in the JRun component of Macromedia ColdFusion web server. Attackers may send overly long HTTP headers to overflow the logging function, enabling an attacker to crash or take control of the web server.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:COLDFUSION:JRUN-SC-PARSE</td>
<td>This signature detects attempts to exploit a vulnerability in the JRun component of Macromedia ColdFusion web server. Attackers may pass a semi-colon character to JRun to expose the script source code and other sensitive files.</td>
<td>low</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:DIR:CRYSTAL-REPORTS</td>
<td>This signature detects attempts to exploit a vulnerability in Microsoft Crystal Reports. Users of Visual Studio .NET 2003, Outlook 2003 with Business Contact Manager, or Microsoft Business Solutions Customer Relationship Management (CRM) 1.2 are affected. Attackers may send a malformed URL to the server to read or write to any file on the server.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:DIR:DEEP-PARAM-TRAVERSE</td>
<td>This signature detects directory traversal attempts within HTTP GET or POST form parameters that extend three or more directories. Attackers may exploit a poorly-written CGI program to access or modify private files.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:DIR:PARAM-TRAVERSE</td>
<td>This signature detects directory traversal attempts within HTTP GET or POST form parameters. Attackers may exploit a poorly-written CGI program to access or modify private files.</td>
<td>low</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:DIR:TRAVERSE-DIRECTORY</td>
<td>This protocol anomaly is an HTTP directory traversal attempt, i.e. /../ or /./. This may indicate an attempt to evade an IDS (DI is not vulnerable). Note that some websites refer to directories in a way that looks like a traversal.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:EXPLOIT:AMBIG-CONTENT-LEN</td>
<td>This protocol anomaly is an HTTP request that has a Content-Length and Transfer-Encoding header. RFC-2616#4.4 specifies that only one of these two headers should be used in an HTTP request.</td>
<td>low</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:EXPLOIT:BLAZIX-JSPVIEW</td>
<td>This signature detects attempts to exploit a vulnerability in the Blazix, a Java-based Web server. Blazix 1.2 and earlier versions are vulnerable. Because Blazix does not strip bad characters (such as '+' and '*') from URL requests, attackers may send a malicious URL to the Web server to view the jsp server side scripts.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:EXPLOIT:BRUTE-FORCE</td>
<td>This protocol anomaly is too many authentication failures (Web pages that require authentication) within a short period of time between a unique pair of hosts.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:EXPLOIT:BRUTE-SEARCH</td>
<td>&quot;This protocol anomaly is multiple 301 (Moved Permanently), 403 (Forbidden), 404 (Not Found) and 405 (Method Not Allowed) errors between a unique pair of hosts within a short period of time. This could indicate that a search robot or a script is methodically searching a Web site for vulnerable directories or CGI scripts. The default maximum number of 301/403/404/405 errors is 16.\n\nAn attack name is:PUBKEY-EXPLOIT. This signature detects attempts to access potentially malicious Web sites. When using Microsoft Internet Explorer, a user can be tricked into visiting a malicious Web site that they believe is benign. Additional IE vulnerabilities may allow the malicious Web site to run scripts in the Local Computer zone, which bypasses security checks on the user’s machine. In your logs for the event, the malicious Web site appears as the destination IP address.\n\n</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------------</td>
</tr>
<tr>
<td>HTTP:EXPLOIT:ILLEGAL-HOST-CHAR</td>
<td>This signature detects illegal characters in a Host header field of an HTTP/1.1 request. Attackers may send an HTTP link, that, when selected by the user, generates an HTTP request to a malicious Web site. In your logs, the destination IP address for the event may be the malicious Web site; however, some foreign Web sites may also trigger this signature, creating a false positive. Per RFC, '_' is not a legal character for a host name.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:EXPLOIT:REALPLAYER-SKIN</td>
<td>This signature detects malicious RealPlayer skin files.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:EXPLOIT:SHOUTCAST-FMT-STR</td>
<td>This signature attempts to exploit a known vulnerability in the Shoutcast streaming audio server. Attackers may gain complete control of the target host.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:EXPLOIT:WIN-MAL-COMP-FILE</td>
<td>This signature detects attempts to exploit a vulnerability in Microsoft Windows native compressed file handler. Attackers may send.zip files with overly long filenames to overflow the file handler and run arbitrary code.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:EXT:GRP-EXT-HTTP</td>
<td>This signature detects GRP files sent over HTTP. GRP files can contain Windows Program Group information, and may be exploited by malicious users to deposit instructions or arbitrary code on a target's system. User involvement is required to activate GRP files; typically they are attached or linked to a harmless-appearing e-mail message.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:EXT:JOB</td>
<td>This signature detects an attempt to download a Microsoft Task Scheduler (.job) file. Opening a malicious .job file in Task Scheduler may allow for arbitrary code execution, leading to system compromise. This vulnerability is present in Microsoft Windows 2000 Service Pack 2 and later. It is also present in Microsoft Windows XP Service Pack 1.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:FRONTPAGE:ADMIN.PWD-REQ</td>
<td>This signature detects attempts to access the Microsoft FrontPage Extensions for UNIX .pwd file that contains sensitive account information.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:FRONTPAGE:DOS-LONGNAME</td>
<td>This signature detects attempts to exploit a known vulnerability in Microsoft Frontpage. Attackers may send a malformed request with an MS-DOS device name to shtml.exe to crash the server.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:FRONTPAGE:FOURDOTS</td>
<td>This signature detects attempts to exploit the '/..../' directory traversal vulnerability in Microsoft FrontPage PWS.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:FRONTPAGE:FP30REG.DLL-OF</td>
<td>This signature detects buffer overflow attempts against Microsoft FrontPage extensions in Windows 2000 and XP. Attackers may execute arbitrary code on the target host.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:FRONTPAGE:SERVICE.PWD-REQ</td>
<td>This signature detects attempts to access the Microsoft FrontPage extensions for UNIX .pwd file which contains sensitive account information.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:HOSTCTRL:THEFT-USER</td>
<td>This signature detects attempts to exploit a vulnerability in the theft-user script supplied with Hosting Controller, a tool that allows Microsoft Windows network administrators to centralize administrative tasks into one interface. Attackers may send a maliciously crafted URL request for theft-user to view arbitrary directories and files on hard drives.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:HOSTCTRL:PERF-EXECUTE</td>
<td>This signature detects attempts by users to download potentially hazardous attachments from MSN Hotmail.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>---------------</td>
</tr>
<tr>
<td>HTTP:IIS:AD-SERVER-CONFIG</td>
<td>This signature detects attempts to download the site.csc configuration file for Microsoft Ad Server. Attackers may access sensitive information.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:IIS:ASP-CODEBROWSER-EXAIR</td>
<td>This signature detects attempts to exploit the Showcode ASP vulnerability in Microsoft IIS.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:IIS:ASP-DOT-NET-BACKSLASH</td>
<td>This signature detects backslash () characters in the URL portion of an HTTP request. Attackers may use a backslash as a directory separator instead of the normal forward slash (/) to bypass the Microsoft IIS ASP.Net authentication capabilities and access protected resources. Note: A poorly configured web server may also display a backslash in a non-malicious URL request.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:IIS:BAT-&amp;</td>
<td>This signature detects attempts to execute a command by specifying a .bat or .cmd extension to a Microsoft Windows Web server.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:IIS:COMMAND-EXEC</td>
<td>This signature detects attempts to exploit Microsoft Windows Web servers. Attackers may send a maliciously crafted url containing the string &quot;cmd.exe&quot; to execute commands on the Web server.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:IIS:COMMAND-EXEC-2</td>
<td>This signature detects attempts to exploit a vulnerability in Microsoft IIS. Attackers may execute arbitrary commands on the Web server.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:IIS:DATA-DISCLOSURE</td>
<td>This signature detects attempts to obtain the sourcecode of Active Server Pages served by Microsoft’s Internet Information Server. In IIS, remote attackers can obtain source code for ASP files by appending &quot;&quot;'::$DATA&quot; to the URL.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:IIS:HEADER-HOST-DOS</td>
<td>This signature detects denial-of-service (DoS) attempts against Microsoft IIS. Attackers may pass maliciously malformed header values to the host to crash the IIS service.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:IIS:NSISLOG-OF</td>
<td>This signature detects buffer overflow attempts against Microsoft Windows Media Services, included with Microsoft Windows 2000 Server SP4. Attackers may send a maliciously crafted HTTP &quot;POST&quot; request to overflow the buffer.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:IIS:ISAPI-IDA-OVERFLOW</td>
<td>This signature detects buffer overflow attempts against Microsoft ISAPI Indexing Service for IIS. Index Server 2.0 and Indexing Service 2000 in IIS 6.0 beta and earlier versions are vulnerable. Attackers may send a long argument to Internet Data Administration (.ida) and Internet Data Query (.idq) files to overflow the buffer in the ISAPI extension (idq.dll) and execute arbitrary commands.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:IIS:ISAPI-IDQ-OVERFLOW</td>
<td>This signature detects buffer overflow attempts against Microsoft ISAPI Indexing Service for IIS. Index Server 2.0 and Indexing Service 2000 in IIS 6.0 beta and earlier versions are vulnerable. Attackers may send a long argument to Internet Data Administration (.ida) and Internet Data Query (.idq) files to overflow the buffer in the ISAPI extension (idq.dll) and execute arbitrary commands.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:IIS:ISAPI-PRINTER-OVERFLOW</td>
<td>This signature detects attempts to execute a buffer overflow in the Microsoft IIS 5.0 .printer ISAPI extension.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:IIS:MALFORMED-HTR-REQUEST</td>
<td>This signature detects malformed .htr requests that may cause a denial-of-service (DoS).</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>-------------------</td>
</tr>
<tr>
<td>HTTP:IIS:MDAC-RDS</td>
<td>This signature detects attempts to exploit the Microsoft Data Access Components (MDAC) Remote Data Services (RDS) component. Attackers may access files and other services.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:IIS:MDAC-RDS-2</td>
<td>This signature detects attempts to exploit the Remote Data Services (RDS) component included in Microsoft Data Access Components (MDAC) using ActiveDataFactory. Microsoft IIS 3.x and 4.x are vulnerable. Attackers may remotely access exposed unsafe methods to execute arbitrary commands.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:IIS:MFC-EXT-OF</td>
<td>This signature detects buffer overflow attempts against Microsoft IIS. A maliciously crafted HTTP request can exploit a buffer overflow condition in mfc42.dll by way of ext.dll. Attackers may gain local access to an IIS server.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:IIS:NEWDSN-FILE-CREATION</td>
<td>This signature detects attempts to create a file on the Web server by exploiting the newdsn.exe vulnerability in Microsoft IIS 3.0.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:IIS:NSIISLOG-CHUNKED-POST</td>
<td>This signature detects chunked POST requests to NSIISLOG.DLL. Attackers may exploit Windows Media Services that have logging enabled, and other vulnerabilities using this method.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:IIS:OUTLOOK-WEB-DOS</td>
<td>This signature detects denial-of-service (DoS) attempts against Microsoft Outlook Web. Attacker may send a long string of '%c' characters as the user name and/or password.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:IIS:PROPFIND</td>
<td>This signature detects attempts to exploit a vulnerability in Microsoft IIS 5.0. Attackers may send malicious 'PROPFIND' requests to the server to crash it.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:IIS:SADMIND-WORM-ACCESS</td>
<td>This signature detects the sadmind/IIS worm attempting to infect Microsoft IIS. The sadmind/IIS worm first exploits a vulnerability in a Solaris system, then attacks Microsoft IIS Web servers using the Web server folder directory traversal exploit.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:IIS:SENSEPOST:EXE</td>
<td>This signature detects attempts to locate sensepost.exe on a Microsoft IIS Web Server. Attackers may use a proof-of-concept hacking tool to break into a vulnerable Web server, then copy cmd.exe to the Web server script directory and rename it sensepost.exe to avoid detection by log viewers. To identify this event, check your Web server logs for details—if the server returned a '200' to the request, your Web server may be compromised.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:IIS:SITE-SERVER-FILE-UPLD</td>
<td>This signature detects attempts to exploit a vulnerability in MS Site Server 2.0 with IIS 4. Attackers may upload content (including ASP) to the target web site and remotely execute commands.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:IIS:WEBDAV:LOCK-OF</td>
<td>This signature detects buffer overflow attempts against Microsoft IIS WebDAV. Attackers may send a maliciously crafted WebDAV URL request that contains 65535 or 65536 bytes to the Web server to execute arbitrary code as the system account.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:IIS:WEBDAV:MALFORMED-REQ1</td>
<td>This signature detects denial-of-service (DoS) attempts against Microsoft IIS 5.0 servers with WebDAV extensions enabled. Attackers may send a maliciously crafted WebDAV SEARCH request in an HTTP request to DoS the Web server.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>-----------</td>
</tr>
<tr>
<td>HTTP:IIS:WEBDAV: MALFORMED-REQ2</td>
<td>This signature detects denial-of-service (DoS) attempts against Microsoft IIS 5.0 servers with WebDAV extensions enabled. Attackers may send a maliciously crafted WebDAV SEARCH request in an HTTP request to DoS the Web server.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:IIS:WEBDAV: SEARCH-OF</td>
<td>This signature detects buffer overflow attempts against Microsoft IIS WebDAV. Attackers may send a maliciously crafted WebDAV URL request that contains 65535 or 65536 bytes to the Web server to execute arbitrary code as the system account.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:IIS:WEBDAV: XML-HANDLER-DOS</td>
<td>This signature detects denial-of-service (DoS) attempts against the WebDAV XML Message Handler in Microsoft IIS. Attackers may send a malicious HTTP request to a WebDAV enabled IIS server to cause it to consume all system resources. A machine reboot is required to resume service.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:INFO: HTTPPOST-GETSTYLE</td>
<td>This signature detects HTTP POST requests with GET parameters. POST requests should not have parameters on the same line as the request method. This may indicate a poorly-written Web application or HTTP tunneling.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:INFO-LEAK: GOAHEAD-PERM</td>
<td>This signature detects attempts to bypass directory permissions set on the /cgi-bin directory of a GoAhead web server. GoAhead WebServer versions 2.1.8 and earlier are vulnerable. Attackers may supply an invalid URL to the server to reveal the contents of certain private directories on the server.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:INFO-LEAK: HTACCESS</td>
<td>This signature detects probes for the .htaccess file, used by the Apache Web server for configuration directives. Attackers may be attempting to gain access to the Web server.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:INFO-LEAK: HTPASSWD-REQUEST</td>
<td>This signature detects attempts to access the .htpasswd file on a Web server.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:INFO-LEAK: VIGNETTE-DIAG</td>
<td>This signature detects attempts to access the diagnostic utility supplied with the Vignette Application server. Because the utility does not use access controls, attackers (or any client) may connect to the utility and access sensitive configuration information.</td>
<td>low</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:INFO-LEAK: VIGNETTE-LEAK</td>
<td>This signature detects attempts to exploit a vulnerability in Vignette Story Server. Vignette Story Server versions 4.1 and 6 are vulnerable. Attackers may expose information about user sessions, server side code, and other sensitive information.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:INFO-LEAK: WEB-INF-DOT</td>
<td>This signature detects attempts to exploit a vulnerability in Windows Web servers with J2EE. Attackers may append a '.' character to a request for the WEB-INF directory (where J2EE class files are typically stored) to bypass directory security and gain access to normally protected files.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:INFO-LEAK: WR850-CONF-DL</td>
<td>This signature detects attempts to download the configuration file from a Motorola WR850G Wireless Router.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:INVALID: INVLD-AUTH-CHAR</td>
<td>This protocol anomaly is an HTTP header with an authorization string that contains an invalid character. The authorization line is decoded using base64.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>-----------</td>
</tr>
<tr>
<td>HTTP:INVALID:INVLD-AUTH-LEN</td>
<td>This protocol anomaly is an HTTP header with an authorization string that has an invalid length (a length that is not a multiple of 4). Because the authorization line is encoded/decoded using base64, the length must be a multiple of 4.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:INVALID:MISSING-REQ</td>
<td>This protocol anomaly is an HTTP header that has no request line or request uniform resource identifier (URI).</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:IRIX:CGI-BIN-WRAP</td>
<td>This signature detects attempts to exploit the wrap CGI script in SGI IRIX. Attackers may list the contents of Web server directories.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:MISC:EMULIVE-ADMIN</td>
<td>This signature detects an attempt to gain unauthorized administrative access to an EmuLive Server4 daemon.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:MISC:HP-PROCURVE-RESET</td>
<td>This signature detects denial-of-service (DoS) attempts against the HP Procurve 4000M switch. Configuration changes for the switch are made via an HTTP-based interface; however, the script that resets the switch after a configuration change does not properly authenticate the IP address that calls the script. Attackers may call the script repeatedly to perform a DoS.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:MISC:MOBY-LENGTH-DOS</td>
<td>This signature detects denial-of-service (DoS) attacks against the Moby NetSuite. Attackers may send a maliciously crafted HTTP POST request that contains an invalid Content-Length field to the host to crash the Web server.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:MISC:MOODLOGIC-CLIENT</td>
<td>This signature detects use of the Mood Logic client. Mood Logic is an MP3 catalogue system that helps users identify and classify MP3s. If your organization prohibits the use of MP3s, use this signature to detect Mood Logic clients.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:MISC:NG-WG602-BACKDOOR</td>
<td>This signature detects attempts to administer a Netgear WG602 using an undocumented administrator username/password that cannot be changed or disabled. Attackers can modify any setting on the WG602 to perform a denial-of-service (DoS) on the Netgear device or circumvent other access control protocols.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:MISC:NOOP-SLIDE-HEAD-OF</td>
<td>This signature detects buffer overflow attempts against Web servers on Intel x86 platforms. Attackers may use the &quot;No-Op Slide&quot; attack to pad the stack with &quot;No Operation&quot; x86 CPU instructions and overwrite the return address.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:MISC:NOOP-SLIDE-REQ-OF</td>
<td>This signature detects buffer overflow attempts against Web servers on Intel x86 platforms. Attackers may use the &quot;No-Op Slide&quot; attack to pad the stack with &quot;No Operation&quot; x86 CPU instructions and overwrite the return address.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:MISC:SHAMBALA-DOS1</td>
<td>This signature detects denial-of-service (DoS) attempts against Evolvable Shambala Server, an FTP, Web, and Chat server. Version 4.5 is vulnerable. Attackers may send a maliciously crafted request to the Web server to cause a DoS.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:MISC:VISNETIC-DOS</td>
<td>This signature detects attempts to exploit a vulnerability in VisNetic WebSite. Versions 3.5.13.1 and earlier are vulnerable. Attackers may send a malicious OPTIONS request to crash the server.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>-------------------</td>
</tr>
<tr>
<td>HTTP:MISC:WR850-WEBSHELL</td>
<td>This signature detects attempts to access a debug mode web shell supplied with the Motorola WR850 Wireless Router. Attackers may use this access exploit in conjunction with an authentication bypass exploit to gain full control over the router.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:NETSCAPE:ENTERPRISE-DOS</td>
<td>This signature detects denial-of-service (DoS) attempts that exploit the Web Publishing REVLOG command in Netscape Enterprise Server 3.x.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:NOVELL:NETWARE-CONVERT.BAS</td>
<td>This signature detects directory traversal attempts on Novell NetWare Web Server 2.x. The convert.bas CGI script allows file retrieval outside of normal Web server context. Attackers may submit the filename and path as a parameter to the script using relative paths (../../) to traverse directories.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OREILLY:WIN-C-SAMPLE-OVFLOW</td>
<td>This signature detects buffer overflow attempts that exploit the win-c-sample.exe sample script vulnerability in O’Reilly Website Pro 2.0 Web server. The script is placed in the /cgi-shl directory off of the Web root by default.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:ACCEPT</td>
<td>DI has detected a suspiciously long Accept header.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:ACCEPT-ENCODING</td>
<td>DI has detected a suspiciously long Accept-Encoding header.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:ACCEPT-LANGUAGE</td>
<td>DI has detected a suspiciously long Accept-Language header.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:ATP-HTTPD-OF</td>
<td>This signature detects buffer overflow attempts against ATPhttp versions 0.4b and earlier. Attackers may send an overly long GET request to the Web server daemon to overflow the buffer.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:AUTHORIZATION</td>
<td>This protocol anomaly is an HTTP authorization header that exceeds the user-defined maximum. The default length is 128.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:AUTH-OVFLW</td>
<td>This protocol anomaly is an HTTP header with an authorization line that exceeds the user-defined maximum. The default authorization line length is 128.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:CHUNK-LEN-OFLW</td>
<td>This protocol anomaly is an HTTP message that has a chunk length in a Transfer-Encoding: chunk request that is greater than 0x7fffffff. Apache servers 1.3 to 1.3.24 and 2.0 to 2.0.36 are vulnerable. Attackers may cause a denial-of-service (DoS) or execute arbitrary code on the server.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:CHUNK-OVERFLOW</td>
<td>This protocol anomaly is an invalid data chunk length in an HTTP request that uses chunked encoding. The chunked encoding transfer method sends data length requests followed by data chunks that match the negotiated data lengths. Attackers may cause a stack overflow and execute arbitrary code on the server.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:CONTENT-ENCODING</td>
<td>DI has detected a suspiciously long Content-Encoding header.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:CONTENT-LANGUAGE</td>
<td>DI has detected a suspiciously long Content-Language header.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:CONTENT-LENGTH</td>
<td>DI has detected a suspiciously long Content-Length header.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:CONTENT-LOCATION</td>
<td>DI has detected a suspiciously long Content-Location header.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>-----------</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:CONTENT-MD5</td>
<td>DI has detected a suspiciously long Content-MD5 header.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:CONTENT-OVERFLOW</td>
<td>This protocol anomaly is a missing line break after a specified data length in an HTTP request using content length transfer. The content length transfer method sends the specified data length in the BODY of the request followed by a line break.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:CONTENT-TYPE</td>
<td>This protocol anomaly is a Content-Type header length that exceeds the user-defined maximum. The default length is 64.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:COOKIE</td>
<td>This protocol anomaly is an HTTP Cookie header length that exceeds the user-defined maximum. The default length is 8192.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:HEADER</td>
<td>This protocol anomaly is an HTTP header field that is too long, and may indicate a buffer overflow attempt.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:HOST</td>
<td>This protocol anomaly is an HTTP Host header length that exceeds the user-defined maximum. The default length is 64.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:HTTPA-OF1</td>
<td>This signature detects buffer overflow attacks against the HTTPa daemon. Attackers may send a maliciously crafted HTTP GET request to the host to overflow the buffer.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:INV-CHUNK-LEN</td>
<td>This protocol anomaly is an invalid chunk length specification in a chunked transfer encoded HTTP request. RFC-2616#6.6.1 specifies that the size of a chunk should be represented using hexadecimal notation.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:JANASRV-VER-OF</td>
<td>This signature detects buffer overflow attempts against JanaServer HTTP Server, an Internet gateway for Windows. JanaServer 2.21 and prior are vulnerable. Attackers may send a maliciously crafted HTTP GET request to overflow the buffer.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:LIBHTTPD-GET-OF</td>
<td>This signature detects buffer overflow attempts against LibHTTPd. LibHTTPd 1.2 and earlier are vulnerable. Attackers may send a maliciously crafted GET request to execute arbitrary code on the host.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:METHOD-GENRC-OF</td>
<td>This signature detects buffer overflow attempts against HTTP request methods. Attackers may send an invalid or long HTTP request to overflow vulnerable buffers on the target Web server.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:NULLHTTPD-ROOT-OF</td>
<td>This signature detects buffer overflow attempts against Null HTTPD. Attackers may remotely send shellcode in a maliciously crafted POST command to gain local access.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:PI3WEB-SLASH-OF</td>
<td>This signature detects denial-of-service (DoS) attempts against PI3Web Server. Attackers may send a URL with more than 354 Slashes (/) to crash the server.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:REFERER</td>
<td>This protocol anomaly is an HTTP Referrer header length that exceeds the user-defined maximum. The default length is 8192.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:SAMBAR-SEARCH</td>
<td>This signature detects buffer overflow attempts against Sambar Server, a free Web server. Attackers may include an oversized HTTP header within a maliciously crafted request to the server to execute arbitrary code.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:SERVER</td>
<td>DI has detected a suspiciously long Server header.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:SET-COOKIE</td>
<td>DI has detected a suspiciously long Set-Cookie header.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:TRANSFER-ENCODING</td>
<td>DI has detected a suspiciously long Transfer-Encoding header.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:OVERFLOW:USER-AGENT</td>
<td>This protocol anomaly is an HTTP User-Agent header length that exceeds the user-defined maximum. The default length is 258.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:ALEXPHP-INCLUDE</td>
<td>This signature detects attempts to exploit a remote file inclusion vulnerability in AlexPHP. Attackers may send a maliciously crafted HTTP request to execute PHP code from a remote server on the host running AlexPHP.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:BLACKBOARD-INC</td>
<td>This signature detects attempts to exploit a vulnerability in the admin.inc.php script that shipped as part of the BlackBoard suite. Attackers may force the admin.inc.php script to include and execute PHP code from a remote source.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:COOLPHP-DIRTRA V</td>
<td>This signature detects directory traversal attempts against CoolPHP. Attackers may use this exploit to execute arbitrary scripts on the PHP server.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:DFORUM-PHP-INC</td>
<td>This signature detects attempts to exploit a vulnerability in D-Forum. D-Forum versions 1.0 through 1.11 are vulnerable. Attackers may exploit header.php3 and footer.php3 to include PHP code from a remote host and execute arbitrary commands.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:FI-DIR-TRAVERSAL</td>
<td>This signature detects attempts to exploit a design vulnerability in PHP/FI. Attackers may remotely access files and directories that are readable by the Web server UID to gather information on the local host and retrieve encrypted user passwords on the system.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:GALLERY:EMBED-AUTH</td>
<td>This signature detects attempts to exploit a vulnerability in Gallery, a Web-based photo album application written in php. Attackers may bypass user authorization to gain administrative privileges.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:GALLERY:HTTP-VARS</td>
<td>This signature detects attempts to exploit a vulnerability in Gallery, a Web-based photo management application. Gallery uses the variables HTTP_POST_VARS, HTTP_GET_VARS, HTTP_COOKIE_VARS, and HTTP_POST_FILES to transfer data between pages, including the GALLERY_BASEDIR variable. Attackers may manually control these variables to include a malicious setting for GALLERY_BASEDIR, enabling them to execute arbitrary PHP code on the Gallery server with the permissions of the HTTP server.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:GALLERY:MAL-INCLUDE</td>
<td>This signature detects attempts to exploit a vulnerability in Gallery online photo gallery software. Attackers may inject malicious PHP code into the software to execute operations on the Web server.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:MANTIS-ARB-EXEC1</td>
<td>This signature detects attempts to exploit a vulnerability in Mantis, an open source Web-based bug tracking system. Mantis 0.17.3 and earlier versions are vulnerable. Attackers may send a maliciously crafted URL to cause the Web server to download PHP code from a remote server, allowing the attacker to execute arbitrary code with the permissions of the user that is running the Web server daemon.</td>
<td>medium</td>
<td>sos5.0.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>HTTP:PHP:MANTIS-ARB-EXEC2</td>
<td>This signature detects attempts to exploit a vulnerability in Mantis, an open source Web-based bug tracking system. Mantis 0.17.3 and earlier versions are vulnerable. Attackers may send a maliciously crafted URL to cause the Web server to download PHP code from a remote server, allowing the attacker to execute arbitrary code with the permissions of the user that is running the Web server daemon.</td>
<td>medium</td>
<td>sos5.0.0</td>
</tr>
<tr>
<td>HTTP:PHP:MLOG-SCREEN</td>
<td>This signature detects attempts to exploit the vulnerable mlog.phtml script. Attackers may remotely access arbitrary files on the Web server.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:NULL-CHAR-IN-TAG</td>
<td>This signature detects attempts to exploit a known vulnerability in the PHP Hypertext Processor (PHP) scripting language used on many Unix/POSIX-based web servers. PHP does not properly check for an encoded NULL character (%00) within parameters passed to it. Because PHP does not properly filter the HTML for malicious content, attackers may post HTML that contains malicious code to a PHP-enabled web site. When other users visit the web site, the malicious code runs on their web browser with credentials allowed for the site by that user.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:PHORUM:ADMIN-PW-CHG</td>
<td>This signature detects attempts to exploit the vulnerable admin.php3 script in Phorum. Attackers may remotely send a maliciously crafted string to the script, change the administrative password of the board without user verification, and access restricted files on the local system.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:PHORUM:READ-ACCESS</td>
<td>This signature detects access to the vulnerable read.php3 script installed with Phorum. Because the script does not validate input, attackers may execute arbitrary SQL statements to modify the database contents, insert new entries, create and drop tables, etc.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:PHORUM:REMOTE-EXEC</td>
<td>This signature detects attempts to exploit a vulnerability in the PHP Phorum bulletin board system. Attackers may remotely execute arbitrary commands with the privileges of the HTTP server.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHPBB:HIGHLIGHT-EXEC</td>
<td>This signature detects attempts to exploit a vulnerability in phpBB. Attackers may send a malformed HTTP request to phpBB to force phpBB to execute arbitrary perl commands on the server with Web server permissions.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHPBB:HIGHLIGHT-EXEC2</td>
<td>This signature detects attempts to exploit a vulnerability in phpBB. Attackers may send a malformed HTTP request to phpBB to force phpBB to execute arbitrary perl commands on the server with Web server permissions.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHPBB:PM_SQL_USR</td>
<td>This signature detects attempts to inject SQL code into a request to phpBB, a popular open-source bulletin board application written in php. Attackers may send a maliciously crafted request that supplies SQL commands to the pm_sql_user parameter, changing database values and escalating client privileges.</td>
<td>low</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHPBB:SEARCH-INJECT</td>
<td>This signature detects attempts to exploit a vulnerability in phpBB, an open-source bulletin board package. The search_id parameter in phpBB is vulnerable to SQL injection. Attackers may query private data (such as hashed passwords) then embed the password in a cookie to gain administrative access to the Web site.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>------------</td>
</tr>
<tr>
<td>HTTP:PHP:PHPDIG-FILE-INC</td>
<td>This signature detects attempts to exploit a vulnerability in PhpDig 1.6. Attackers may include a malicious 'relative_script_path' parameter in a direct request to the config.php script; this request causes the server to download php code from remote location and execute it. Attackers may execute arbitrary code on the server with permissions of the web server.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:PHPLIB-REMOTE-EXEC</td>
<td>This signature detects attempts to exploit a vulnerability in PHPLIB, a code library that provides support for managing sessions in Web applications. Attackers may remotely submit maliciously crafted Web requests to cause the application to fetch and execute scripts from another host, allowing local access to the Web server.</td>
<td>medium</td>
<td>sos5.0.0,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:PHPMYADMIN:SVR-PARAM</td>
<td>This signature detects attempts to exploit a vulnerability in PHPMyAdmin. Attackers may use HTTP form parameters to remotely provide mysql server configuration data. This attack is typically one stage in a multi-stage exploit attempt.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:PHPNUKE:CID-SQL-INJECT</td>
<td>This signature detects attempts to exploit a vulnerability in PHP-Nuke. Attackers may execute arbitrary SQL commands on a Web server.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:PHPNUKE:MODULES-DOS</td>
<td>This signature detects attempts to exploit a SQL injection vulnerability in the modules.php script that ships with PHPNuke. PHPNuke 6.0 and earlier are vulnerable. Attackers may produce a process that increases system load on the server, making it unusable until the process is killed.</td>
<td>medium</td>
<td>sos5.0.0,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:PHPROJEKT-INC</td>
<td>This signature detects attempts to exploit a vulnerability in the authform.inc.php script included in the PHProjekt package. Attackers may supply a remote location in the 'path_pre' input parameter to force the target to download and execute arbitrary PHP code from the remote location.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:PHPWEB-REMOTE-FILE</td>
<td>This signature detects attempts to exploit a vulnerability in phpWebsite. Version 0.8.2 and earlier are vulnerable. Attackers may specify a remote file location for file inclusion to cause phpWebsite to execute arbitrary PHP code; attackers may execute commands with HTTP daemon user permissions.</td>
<td>high</td>
<td>sos5.0.0,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:PMACHINE-INCLUDE</td>
<td>This signature detects attempts to exploit a vulnerability in pMachine, an online publishing application. pMachine version 2.2.1 and other versions are vulnerable. Attackers may send a malicious HTTP request to force the pMachine Web server to execute PHP code from a remote server; commands are executed with web server privileges.</td>
<td>high</td>
<td>sos5.0.0,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:POPPER-OPEN-ADMIN</td>
<td>This signature detects attempts to exploit a vulnerability in popper_mod 1.2.1, a Web-based PHP POP3 email client based on Qpopper. Popper_mod relies on htaccess authentication to authenticate administrators; if htaccess is not used to protect admin access, popper_mod does not authenticate administrators. Attackers may browse to the /mail/admin directory to access the administration PHP script and view a complete list of user accounts and passwords, delete accounts, modify accounts, and edit settings.</td>
<td>high</td>
<td>sos5.0.0,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>-------------------</td>
</tr>
<tr>
<td>HTTP:PHP:REDHAT-PIRANHA-PASSWD</td>
<td>This signature detects attempts to exploit the vulnerable passwd.php3 cgi-bin script in the Piranha virtual server package (RedHat Linux 6.2). Because the script does not validate input properly, attackers may authenticate to the Piranha package with the effective ID of the Web server and execute arbitrary commands.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:SILENT-STORM-ADMIN</td>
<td>This signature detects attempts to raise the privileges on an account for the Silent Storm PHP Portal.</td>
<td>low</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:UPLOAD-LOCATION</td>
<td>This signature detects a maliciously crafted HTTP POST request. Attackers may use a directory traversal attack within the Content-Disposition field of a POST request to force PHP to execute arbitrary code.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:VBULL-CAL-EXEC</td>
<td>This signature detects attempts to exploit a vulnerability in the calender.php script that is included with the vBulletin package. Attackers may run the vbull.c exploit to execute arbitrary commands with Web Server user permissions.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:WOLTAB-SQL-INJ</td>
<td>Any user on the bulletin board can compromise any other user's account by exploiting a vulnerability in board.php. Board.php does not perform proper input validation, and therefore is subject to executing user-supplied SQL statements. This is known to affect WolTab Burning Board 2.0 RC 1 and earlier versions.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:YABBSE-PKG-EXEC</td>
<td>This signature detects attempts to exploit a vulnerability in Packages.php in YabbSE. YabbSE 1.5.0 and earlier are vulnerable. Attackers may include remote malicious code in Packages.php to include remote malicious code to execute arbitrary commands with Web server privileges.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:YABBSE-SSI-INCLUDE</td>
<td>This signature detects attempts to exploit a vulnerability in YabbSE, a PHP/MySQL port of the forum software YaBB (yet another bulletin board). YabbSE versions 1.5.2 and earlier are vulnerable. Attackers may include PHP code in a maliciously crafted URL request; when YabbSE receives the request it runs the PHP code, enabling the attacker to execute arbitrary commands on the server.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PHP:ZENTRACK-CMD-EXEC</td>
<td>This signature detects attacks against the PHP-based zenTrack CRM system. A vulnerability exists in the header.php that holds zenTrack configuration settings. It allows remote command execution as the webserver process privilege. This applies to zenTrack 2.4.1 and below.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PKG:ALLAIRE-JRUN-DOS</td>
<td>This signature detects an attempt to launch a denial-of-service (DoS) in Allaire JRun 3.0/3.1. Attackers may send a long string of &quot;.&quot; characters after the /servlet/ prefix in the URL to cause the server to interpret the URL as a very large tree of non-existent directories and to consume system resources.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PKG:DB4WEB-FILE-ACCESS-LIN</td>
<td>This signature detects attempts to exploit a vulnerability in DB4Web (R) Application Server for Windows. Attackers may use a Web browser to download arbitrary files to the target host and obtain system information such as passwords.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PKG:EWave-Servlet-DOS</td>
<td>This signature detects denial-of-service (DoS) attempts against the eWave Servlet JSP. Attackers may remotely send URL requests to cause the Servlet engine to terminate abruptly.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>-----------</td>
</tr>
<tr>
<td>HTTP:PKG:_MOUNTAIN-ORDR-DSCLSR</td>
<td>This signature detects attempts to exploit a vulnerability in Mountain Network Systems Webcart software. Attackers may remotely execute arbitrary commands on the server.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PKG:WEBGAIS-REMOTE-EXEC</td>
<td>This signature detects attempts to exploit the webSendmail script in WebGais. Attackers may execute arbitrary commands on the Web server.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:PROXY:DOUBLE-AT-AT</td>
<td>This signature detects URLs that contain multiple @ characters. Squid/2.3.STABLE5 is vulnerable. Internet Explorer users may use these malicious URLs to evade web proxies and gain direct access to the internet.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:REQERR:HEADER-INJECT</td>
<td>This signature detects attempts to exploit an input validation vulnerability in HTTP. Attackers may use encoded CR/LF (carriage return/line feed) characters in an HTTP response header to split HTTP responses into multiple parts, enabling them to misrepresent web content to the recipient.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:REQERR:REQ-INVALID-FORMAT</td>
<td>This protocol anomaly is an invalid HTTP request format, such as a request that begins before a previous one ends.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:REQERR:REQ-LONG-UTF8CODE</td>
<td>This protocol anomaly is an HTTP request with an exceedingly long UTF8 codes. This may be an attempt to overflow a portion of the Web server, or that a script is being made available to the Web server.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:REQERR:REQ-MALFORMED-URL</td>
<td>This protocol anomaly is a malformed URL, such as a Unicode encoded field with non-hex digits or an encoded NULL byte.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:SAVANT:Get-DOT1</td>
<td>This signature detects denial-of-service (DoS) attempts against the Savant HTTP server. Savant HTTP server 3.0 and earlier versions are vulnerable. Attackers may send a maliciously crafted HTTP GET request to the Web server to crash the server and create a DoS.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:SPYWARE:DOWNLOAD-ACCEL</td>
<td>This signature detects the use of Download Accelerator, a spyware application.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:SPYWARE:GATOR</td>
<td>This signature detects the use of Gator, a spyware application.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:SPYWARE:NEW-DOT-NET</td>
<td>This signature detects the use of New.net, a spyware application.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:SQL:INJECTION:CMD-CHAIN-1</td>
<td>This signature detects a SQL command sequence in a URL. Because SQL commands are not normally used in HTTP connections, this may indicate a SQL injection attack. However, it may also be a false positive.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:SQL:INJECTION:CMD-CHAIN-2</td>
<td>This signature detects a long SQL command sequence in a URL. Because SQL commands are not normally used in HTTP connections, this may indicate a SQL injection attack.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:SQL:INJECTION:CMD-IN-URL</td>
<td>This signature detects SQL commands within a URL. Because SQL commands are not normally used in HTTP connections, this may indicate a SQL injection attack. However, it may be a false positive.</td>
<td>low</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:SQL:INJECTION:FACTO-CMS</td>
<td>This signature detects attempts to exploit a vulnerability in the FactoSystem Content Management System (CMS). Attackers may introduce instructions into a SQL query to create a non-authorized CMS account.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>HTTP:SQL:INJECTION:GENERIC</td>
<td>This signature detects specific characters, typically used in SQL, within an HTTP connection. Because these characters are not normally used in HTTP, this may indicate a SQL injection attack. However, it may be a false positive. Some attempts at Cross Site Scripting attacks will also trigger this signature.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:SQL:INJECTION:POSTNUKE</td>
<td>This signature detects directory traversal attempts against the modules.php script included with PostNuke. PostNuke versions 0.723 and earlier are vulnerable. Attackers may send a maliciously crafted request to the modules.php to traverse the directory structure and execute SQL queries to the PostNuke database.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:SQL:INJECTION:WS2000</td>
<td>This signature detects SQL injection attempts against a WebStore2000 server. Attackers may inject SQL code into the Item_ID parameter of a maliciously crafted request, enabling them to execute arbitrary SQL commands on the WebStore2000 server.</td>
<td>medium</td>
<td>sos5.1.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:STC:ACROBAT-EXT-OF</td>
<td>This signature detects buffer overflow attempts against Adobe Acrobat Reader. A malicious HTTP server may host an Adobe Acrobat file with an overly long extension; when a client opens this file in Adobe Acrobat Reader, the file triggers a buffer overflow, enabling the server to execute arbitrary code on the client.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:STC:ACROBAT-UUEXEC</td>
<td>This signature detects a maliciously crafted PDF file downloaded via HTTP. Attackers may insert certain shell metacharacters at the beginning of a uuencoded PDF file to force Adobe Acrobat to execute arbitrary commands upon loading the file.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:STC:EICAR-DOWNLOAD</td>
<td>This signature detects the EICAR antivirus test file downloaded via HTTP.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:STC:EXCEL-CELL-OF</td>
<td>This signature detects a maliciously crafted Microsoft Excel file downloaded via HTTP. Attackers may supply an Excel document that contains an overly long Cell Length field to overflow the buffer and execute arbitrary code on the client.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:STC:IE:CONT-LOC-ZON-BYPASS</td>
<td>This signature detects attempts to circumvent a security zone feature that warns when executable files are downloaded. WindowsXP Service Pack 2 and Internet Explorer 6 are vulnerable. Attackers may trick a user into downloading a file that the user did not know was executable. Similarly, viruses and worms may use this method to download themselves onto target computers.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:STC:IE:EXEC-CMD-FILE-SPOOF</td>
<td>This signature detects attempts to exploit a vulnerability in the way that Internet Explorer handles the javascript execCommand function. Attackers may trick a user into saving a file that the user thinks is HTML, but is actually an executable file.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:STC:WINAMP:CDDA-OF</td>
<td>This signature detects the download of a maliciously crafted WinAmp playlist file. Using WinAmp to open this file may execute arbitrary code.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:STC:WINAMP:CDDA-OF2</td>
<td>This signature detects the download of a maliciously crafted WinAmp playlist file. Using WinAmp to open this file may execute arbitrary code.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>HTTP:TOMCAT:JSP-AS-HTML</td>
<td>This signature detects attempts to exploit a vulnerability in Apache Tomcat. Apache Tomcat 3.3.1 and earlier are vulnerable. Attackers may send a maliciously crafted URL to cause the server to parse a .jsp file as HTML code and display the JSP code, allowing attackers to retrieve normally inaccessible files.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:TOMCAT:SERVLET-DEVICE-DOS</td>
<td>This signature detects denial-of-service (DoS) attempts against Apache Group Tomcat Server. Attacker may request a device name from the /examples/servlet directory to render the server inaccessible. This signature also detects attempts to run neuter.c and similar exploits.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:TUNNEL:ALTNET-OVER-HTTP</td>
<td>This signature detects attempts to connect to an AltNet server over HTTP. AltNet is a component of Kazaa, a common Peer to Peer file sharing system. Users may be attempting to download files.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:TUNNEL:CHAT-AOL-IM</td>
<td>This signature detects AOL Instant Messenger Proxy over HTTP. Users may use proxy connections over the HTTP port to circumvent firewall policies.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:TUNNEL:CHAT-MSN-IM</td>
<td>This signature detects MSN Instant Messenger over HTTP. Users may use proxy connections over the HTTP port to circumvent firewall policies.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:TUNNEL:CHAT-YIM</td>
<td>This signature detects Yahoo Instant Messenger Proxy over HTTP. Users may use proxy connections over the HTTP port to circumvent firewall policies.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:TUNNEL:HTTPTUNNEL-URL</td>
<td>This signature detects traffic from the HTTPTunnel utility. HTTPTunnel masquerades a network session in HTTP traffic.</td>
<td>low</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:TUNNEL:KAZAA-OVER-HTTP</td>
<td>This signature detects attempts to connect to a Kazaa server over HTTP. Kazaa is a common Peer to Peer file sharing system. Users may be attempting to download files.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:TUNNEL:SSH</td>
<td>This signature detects SSH over HTTP. Attackers may send SSH over the HTTP port to circumvent firewall policies.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:TUNNEL:TELNET</td>
<td>This signature detects Telnet over HTTP. Attackers may send Telnet over the HTTP port to circumvent firewall policies.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:WASD:CONF-ACCESS</td>
<td>This signature detects attempts to exploit a vulnerability in the WASD HTTP Server for OpenVMS. Default installations of 1.0 and earlier are vulnerable. Attackers may download the configuration file for the server and obtain information on the ACL and internal directory structure.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:WASD:DIR-TRAV</td>
<td>This signature detects directory traversal attempts against WASD HTTP Server for OpenVMS. WASD version 1.0 and earlier are vulnerable. Attackers may navigate to any directory on the server.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:WEBLOGIC:URL-REVEAL-SRC</td>
<td>This signature detects attempts to exploit a vulnerability in Bea Weblogic. Version V6.1 Service Pack 2 on Windows 2000 Server is vulnerable. Attackers may append the string &quot;%00x&quot; to a URL request to read the contents of a .jsp file.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:WEBLOGIC:WEBROOT</td>
<td>This signature detects attempts to exploit a vulnerability in Bea Weblogic. Version V6.1 Service Pack 2 on Windows 2000 Server is vulnerable. Attackers may append the string &quot;%00.jsp&quot; to a normal .html request, causing a compiler error that prints the path to the physical web root.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>-----------</td>
</tr>
<tr>
<td>HTTP:WEBPLUS:DIR-TRAVERSAL</td>
<td>This signature detects attempts to exploit the input validation vulnerability in the main CGI in TalentSoft Web+, an e-commerce storefront provider. Attackers may pass a script variable that specifies a filepath to the webpsvr daemon, and gain access to any file on the system that the UID of the Web server has access to.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:WEBSPHERE:VER-DOS</td>
<td>This signature detects denial-of-service (DoS) attempts against the caching proxy in IBM WebSphere Edge Server. Version 2.0 is vulnerable. Attackers may send a maliciously crafted HTTP GET request that does not have a proper version identifier to crash the proxy service and render the proxy unusable.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:WIN-CMD:WIN-CMD-EXE</td>
<td>This signature detects the Windows command 'cmd.exe' within a URL. This command does not normally appear in a URL, and may indicate an attempt to compromise the system.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:WIN-CMD:WIN-RGUEST</td>
<td>This signature detects the Windows command 'rguest.exe' within a URL. This command does not normally appear in a URL, and may indicate an attempt to compromise the system.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:WIN-CMD:WIN-WGUEST</td>
<td>This signature detects the Windows command 'wguest.exe' within a URL. This command does not normally appear in a URL, and may indicate an attempt to compromise the system.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:XSS:HDR-REFERRER</td>
<td>This signature detects attempts to exploit a cross-site scripting vulnerability. Attackers may embed malicious HTML tags within the HTTP Referrer header; because some web servers and server-side applications parse this data incorrectly, attackers can successfully execute a cross-site scripting attack.</td>
<td>low</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>HTTP:XSS:HTML-SCRIPT-IN-URL-PRM</td>
<td>This signature detects attempts at cross site scripting attacks. Attackers may create a malicious Web site that includes HTML embedded in the hyperlinks, which might violate site security settings. Attackers may then view the Web cookies from your computer; Web cookies typically contain sensitive information such as usernames, passwords, credit card numbers, social security numbers, bank accounts, etc.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:XSS:HTML-SCRIPT-IN-URL-PTH</td>
<td>This signature detects cross site scripting attacks. Attackers may create a malicious Web site that includes HTML embedded in the hyperlinks, which might violate site security settings. Attackers may then view the Web cookies from a target computer. Web cookies typically contain sensitive information such as usernames, passwords, credit card numbers, social security numbers, and bank account numbers.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>HTTP:XSS:URL-IMG-XSS</td>
<td>This signature detects HTML <code>&lt;img&gt;</code> tags in URLs that include Javascript. Because <code>&lt;img&gt;</code> tags should never be present in URLs, the presence of Javascript in such a URL is a clear indication of a Cross-Site Scripting (XSS) attack. XSS attacks are typically Web browser-independent.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>IMAP:FAILURE:BRUTE-FORCE</td>
<td>This protocol anomaly is multiple login failures within a short period of time between a unique pair of hosts.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>IMAP:IPSWITCH:DELE-OF</td>
<td>This signature detects buffer overflow attempts against IPSwitch IMAP server. Attackers may send an overly long delete command (DELE) to overflow the buffer and take complete control of the server.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>IMAP:OVERFLOW:COMMAND</td>
<td>This protocol anomaly is an IMAP command that is too long. This may indicate a buffer overflow attempt.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>IMAP:OVERFLOW:FLAG</td>
<td>This protocol anomaly is an IMAP flag that is too long. This may indicate a buffer overflow attempt.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>IMAP:OVERFLOW:IMAP4-LSUB-OF</td>
<td>This signature detects buffer overflow attempts against the IMAP package included with several Linux distributions. Attackers may send a long string to the IMAP package to execute code with daemon-level permissions.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>IMAP:OVERFLOW:LINE</td>
<td>This protocol anomaly is an IMAP line (from the client to the server) that is too long. This may indicate a buffer overflow attempt. NOTE: Long lines are parsed, which may generate other IMAP overflow errors.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>IMAP:OVERFLOW:LIT_LENGTH_OFLOW</td>
<td>This protocol anomaly is an IMAP literal that specifies more octets than the user-defined maximum. A literal is a sequence of zero or more octets. The default maximum number of octets is 65535.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>IMAP:OVERFLOW:MAILBOX</td>
<td>This protocol anomaly is an IMAP mailbox name that is too long. This may indicate a buffer overflow attempt.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>IMAP:OVERFLOW:PASS</td>
<td>This protocol anomaly is an IMAP user password that is too long. This may indicate a buffer overflow attempt.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>IMAP:OVERFLOW:REFERENCE</td>
<td>This protocol anomaly is an IMAP reference field that is too long. This may indicate a buffer overflow attempt.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>IMAP:OVERFLOW:TAG</td>
<td>This protocol anomaly is an IMAP tag field that is too long. This may indicate a buffer overflow attempt.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>IMAP:OVERFLOW:USER</td>
<td>This protocol anomaly is an IMAP user name that is too long. This may indicate a buffer overflow attempt.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>IMAP:REQERR:INVALID_LITERAL_LEN</td>
<td>This protocol anomaly is a literal that specifies a number of octets containing a character that is not 0 or 9.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>IMAP:REQERR:REQ-INVALID-TAG</td>
<td>This protocol anomaly is an invalid IMAP tag, i.e., a tag that begins with a white space or contains non-alphanumeric characters. This may indicate a non-standard IMAP client or command line access to an IMAP server.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>IMAP:REQERR:REQ-UNEXPECTED-ARG</td>
<td>This protocol anomaly is an IMAP command with too many arguments. This may indicate a non-standard IMAP client or command line access to an IMAP server.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
<th>Severity</th>
<th>Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS-RPC:DCOM:SVRNAME-2LONG</td>
<td>This protocol anomaly is a DCOM servername that is longer than 32 octets in unicode.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>MS-RPC:EPDUMP-SCAN</td>
<td>This anomaly detects a client enumerating MSRPC endpoints on a windows server. This may indicate a probing scan prior to a more sophisticated attack.</td>
<td>low</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>MS-RPC:ERR:CL-PTYPE-IN-CO-PDU</td>
<td>This protocol anomaly is an MSRPC connection-oriented message with a packet type that is allowed only in Connectionless PDUs.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>MS-RPC:ERR:CO-PTYPE-IN-CL-PDU</td>
<td>This protocol anomaly is a connectionless MSRPC message with a packet type that is allowed only in connection-oriented PDUs.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>MS-RPC:ERR:EPM-INV-LHS-LEN</td>
<td>This protocol anomaly is an EPM message with an LHS length that is larger than the rest packet length.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>MS-RPC:ERR:EPM-INV-OP-NUM</td>
<td>This protocol anomaly is an invalid EPM operation number.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>MS-RPC:ERR:EPM-INV-RHS-LEN</td>
<td>This protocol anomaly is an EPM message with an RHS length that is larger than the rest packet length.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>MS-RPC:ERR:EPM-INV-TOWER-LEN</td>
<td>This protocol anomaly is an EPM message with a tower length that is larger than 8192 bytes, or larger than the rest fragment length.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>MS-RPC:ERR:EPM-WRONG-LHS-LEN</td>
<td>This protocol anomaly is an EPM packet with a UUID LHS length that is not equal to 19.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>MS-RPC:ERR:EPM-WRONG-RHS-LEN</td>
<td>This protocol anomaly is an EPM message with an RHS length that is larger than the rest packet length.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>MS-RPC:ERR:EPM-WRONG-TOWER-LEN</td>
<td>This protocol anomaly is an EPM message with a tower length that is inconsistent with message’s LHS and RHS lengths.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>MS-RPC:ERR:FRAG-BIGGER-THEN-NEG</td>
<td>This protocol anomaly is a MSRPC fragment length that is larger than the negotiated maximum.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>MS-RPC:ERR:FRAG-LEN-TOO-SMALL</td>
<td>This protocol anomaly is an MSRPC fragment length that is less than the common header length.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>MS-RPC:ERR:INV-AUTH-LEN</td>
<td>This protocol anomaly is an MSRPC message with an authentication length that is larger than the entire MS-RPC message payload length.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>MS-RPC:ERR:INV-AUTH-PAD-LEN</td>
<td>This protocol anomaly is an MSRPC message with authentication padding length plus authentication section length that is larger than the entire MSRPC message payload length.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>MS-RPC:ERR:INV-PTYPE</td>
<td>This protocol anomaly is an MSRPC message that contains an invalid packet type value.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>MS-RPC:ERR:LEN-CONFLICT</td>
<td>This protocol anomaly is an MSRPC connectionless message with a fragment length that conflicts with the common header length and the whole message length.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>MS-RPC:ERR:RESPONSE-NO-REQ</td>
<td>This protocol anomaly is an MSRPC response that precedes the request.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>MS-RPC:ERR:SHORT-MSG</td>
<td>This protocol anomaly is an incomplete MSRPC message.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>MS-RPC:LOC-SVC-OF</td>
<td>This signature detects attempts to exploit a flaw in the Windows DCE RPC Locator service. This service is turned on by default on all Windows NT 4 and Windows 2000 Domain Controllers, or can be turned on manually on all Windows NT, 2000, and XP systems. Attackers can deny the service of the locator, causing network-wide outages, or take control of the service and run code of choice.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>MS-RPC:LSASS:MAL-OPCODE</td>
<td>This signature detects attempts to exploit a known vulnerability in Microsoft Windows LSASS (Local Security Authority Subsystem Service). Attackers may remotely run arbitrary code on the target system. Note: This vulnerability is exploited by many worms.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------</td>
<td>----------</td>
</tr>
<tr>
<td>MS-RPC:LSASS:OVERSIZED-FRAG</td>
<td>This signature detects attempts to remotely attack a known vulnerability in the Microsoft Windows LSASS (Local Security Authority Subsystem Service). A successful attack could run code of an attacker’s choice on the target system. By supplying an oversized fragment to the LSASS service, a buffer can be overflowed that can result in remote code execution.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>MS-RPC:MSRPC-ISYSACTIVATE-RACE</td>
<td>This protocol anomaly is too many DCE/RPC ISystemActivate requests. Excessive requests can cause a denial-of-service (DoS) in the RPCSS module.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>MS-RPC:NOOP-SLIDE-RPC-REQ</td>
<td>This signature detects Unicode NOOP sleds in an RPC request. Because these patterns are usually malicious, they might indicate an attack.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>MS-RPC:SAMR-ACCESS-DENIED</td>
<td>This signature detects failed attempts to connect to the Security Account Manager Remote (SAMR) service on Windows. Attackers may be probing your server for vulnerabilities, as a successful login to this service provides important information such as administrator account details, default domain names, open users, and active groups. However, because system administrators also use the SAMR service legitimately, this signature may also detect non-malicious activity.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>MS-RPC:SAMR-ACCESS-REQUEST</td>
<td>This signature detects attempts to connect to the Security Account Manager Remote (SAMR) service on Windows. Attackers may be probing your server for vulnerabilities, as a successful login to this service provides important information such as administrator account details, default domain names, open users, and active groups. However, because system administrators also use the SAMR service legitimately, this signature may also detect non-malicious activity.</td>
<td>low</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>MS-RPC:WKST-SVC-OFLOW</td>
<td>This protocol anomaly is a suspiciously long argument for the NetrValidateName, NetrValidateName2, or NetrAddAlternateComputerName functions requested using a named-pipe transaction. An unauthenticated user may exploit this vulnerability on Windows 2000/XP servers to execute arbitrary code with system-level privileges.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>NETBIOS:ACCESS:ADMIN</td>
<td>This signature detects attempts to exploit a null session vulnerability in NETBIOS SMB protocols. Attackers may initiate SMB sessions with no user name or password, obtain the remote admin share on the server, and use this information to plan further attacks.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>NETBIOS:ACCESS:C-DRIVE</td>
<td>This signature detects attempts to exploit a null session vulnerability in NETBIOS SMB protocols. Attackers may initiate SMB sessions with no user name or password, obtain the C Drive share on the server, and use this information to plan further attacks.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>NETBIOS:ACCESS:D-DRIVE</td>
<td>This signature detects attempts to exploit a null session vulnerability in NETBIOS SMB protocols. Attackers may initiate SMB sessions with no user name or password, obtain the D Drive share on the server, and use this information to plan further attacks.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>NETBIOS:NBDS:BAD_LABEL_FORMAT</td>
<td>This protocol anomaly is label for the second level encoding of a Netbios name that contains a pointer.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-------------</td>
<td>--------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>NETBIOS:NBSD:INVALID:1STLVL_ENC</td>
<td>This protocol anomaly is an invalid first level encoding of a Netbios name.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>NETBIOS:NBSD:INVALID:DGM_LEN</td>
<td>This protocol anomaly is a Netbios datagram header with a DGM_LENGTH field value that is bigger than the packet length.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>NETBIOS:NBSD:INVALID:HDR_FLGS</td>
<td>This protocol anomaly is a Netbios datagram header with a FLAGS field that contains non-zero values for bits 0-3.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>NETBIOS:NBSD:INVALID:LABEL_LEN</td>
<td>This protocol anomaly is a label for the second level encoding of a netbios name; the label length is larger than 63, or the label is the first label and the length is not 32.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>NETBIOS:NBSD:INVALID:MSG_TYPE</td>
<td>This protocol anomaly is a Netbios datagram header with a MSG_TYPE field value that is invalid.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>NETBIOS:NBSD:INVALID:PROTO</td>
<td>This protocol anomaly is a Netbios message with a USER_DATA section that is less than the size of SMB header, or the protocol field of the SMB header does not start with 0xff 'S' 'M' 'B'.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>NETBIOS:NBSD:OVERFLOW:MSG</td>
<td>This protocol anomaly is a Netbios datagram that is bigger than 1064.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>NETBIOS:NBSD:OVERFLOW:NAME</td>
<td>This protocol anomaly is a Netbios name that is longer than 255.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>NETBIOS:NBNS:C2S_AA_FLAG</td>
<td>This protocol anomaly is query message with an NM_FLAGS field containing an authoritative answer flag that is set.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>NETBIOS:NBNS:C2S_RESPONSE</td>
<td>This protocol anomaly is query message with an OPCODE field containing an response flag that is set.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>NETBIOS:NBNS:CLASS-UNKNOWN</td>
<td>This protocol anomaly is an invalid value in the QUESTION_CLASS field of the question section or in the RR_CLASS field of the resource record header.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>NETBIOS:NBNS:INVALID:FIRST-ENC</td>
<td>This protocol anomaly is an invalid first level encoding of a Netbios name.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>NETBIOS:NBNS:INVALID:HDR-CNT</td>
<td>This protocol anomaly is a 1) a query message with ARCOUNT (answer count) or NSCOUNT (number of records in the authority section of a name service packet) fields of the header that are not zero, or 2) a response message with a QDCOUNT (number of entries in the question section) that is not zero.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>NETBIOS:NBNS:INVALID:HDR-OPCODE</td>
<td>This protocol anomaly is a header with an OPCODE field value that is not 0, 5, 6, 7, or 8.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>NETBIOS:NBNS:INVALID:HDR-Z</td>
<td>This protocol anomaly is a Netbios name header with a NM_FLAGS field that contains non-zero values for bit 4 or bit 5.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>NETBIOS:NBNS:INVALID:LABEL-LEN</td>
<td>This protocol anomaly is a label for the second level encoding of a Netbios name that has a label length larger than 63, or the label is the first label and the length is not 32.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>NETBIOS:NBNS:INVALID:NAME-FLGS</td>
<td>This protocol anomaly is a Netbios name header with a NM_FLAGS field that contains non-zero values for bits 3-15.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>NETBIOS:NBNS:INVALID:PTR</td>
<td>This protocol anomaly is a pointer offset in the second level encoding of a Netbios name that exceeds the message length (the pointer is pointing out of the message).</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>NETBIOS:NBNS:INVALID:RRNB-FLG</td>
<td>&quot;This protocol anomaly is a type node status response message&quot;</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>NETBIOS:NBNS:NAME_TOO_LONG</td>
<td>This protocol anomaly is a Netbios name that is longer than 255.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>NETBIOS:NBNS:POINTER_LOOP</td>
<td>This protocol anomaly is a second level encoding of a Netbios name that contains more nested pointers than the user-defined maximum. Default setting for the sc_nbname_pointer_loop_limit is 8.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>NETBIOS:NBNS:RESCODE:FORMAT_ERR</td>
<td>This protocol anomaly is Netbios name response with an RCODE that indicates the request has an invalid format.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>NETBIOS:NBNS:S2C_QUERY</td>
<td>This protocol anomaly is a Netbios name response header with an OPCODE field that contains an unset response bit.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>NETBIOS:NBNS:SHORT_MSG</td>
<td>This protocol anomaly is a Netbios name message that is shorter than expected.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>NETBIOS:NBNS:TYPE_UNKNOWN</td>
<td>This protocol anomaly is an invalid value in 1) the QUESTION_TYPE field in the question section or 2) the RR_TYPE field in the resource record header.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:AUDIT:GNUTELLA-BYE-TTL</td>
<td>This protocol anomaly is a Gnutella BYE message that does not contain a TTL of 1 and a HOPS of 0.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:AUDIT:GNUTELLA-EOL</td>
<td>This protocol anomaly is a a Gnutella message that does not use the end-of-line (EOL) terminator characters \texttt{&lt;CR&gt;&lt;LF&gt;}</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:AUDIT:GNUTELLA-HDR-ATRB</td>
<td>This protocol anomaly is a Gnutella message with a header line that does not have a value for an attribute; a blank space exists after the attribute colon.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:AUDIT:GNUTELLA-HTTP-GET</td>
<td>This protocol anomaly is a Gnutella GET command that does not use the expected syntax. Correct syntax is: \texttt{GET /get/&lt; File Index&gt;/&lt; File Name&gt; HTTP/1.1&lt; CR&gt;&lt; LF&gt;}.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:AUDIT:GNUTELLA-LINE</td>
<td>This protocol anomaly is a Gnutella message with a line length that exceeds the user-defined maximum number of bytes. The default line length is 2048.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:AUDIT:GNUTELLA-MESSAGE</td>
<td>This protocol anomaly is a Gnutella message with a payload type that is not defined in the Gnutella RFC.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:AUDIT:GNUTELLA-MSG</td>
<td>This protocol anomaly is a Gnutella message with a payload length that exceeds 4096 bytes.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:AUDIT:GNUTELLA-OK-RESP</td>
<td>This protocol anomaly is a Gnutella client response that does not use the expected syntax. Correct syntax for Gnutella 0.6 is: \texttt{GNUTELLA/0.6 200 OK&lt; CR&gt;&lt; LF&gt;}.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:AUDIT:GNUTELLA-PING-LEN</td>
<td>This protocol anomaly is a Gnutella 0.4 PING message that has a non-zero payload length.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:AUDIT:GNUTELLA-PONG-LEN</td>
<td>This protocol anomaly is a Gnutella PONG message that has an invalid payload length. Gnutella 0.4 PONG messages should have exactly 14 bytes; Gnutella 0.6 PONG messages should have a minimum of 14 bytes.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:AUDIT:GNUTELLA-PUSH-LEN</td>
<td>This protocol anomaly is a Gnutella PUSH message with a payload length that is less than 26 bytes.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:AUDIT:GNUTELLA-QUERY</td>
<td>This protocol anomaly is a Gnutella QUERY message with a payload length that exceeds the user-defined maximum number of bytes. The default line length is 256.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>P2P:AUDIT:GNUTELLA-RTABLE-UPD</td>
<td>This protocol anomaly is a Gnutella ROUTE_TABLE_UPDATE message with a payload length of 0 bytes.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:AUDIT:GNUTELLA-SEARCH</td>
<td>This protocol anomaly is a Gnutella message with a search criteria field that does not end with a NULL character.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:AUDIT:GNUTELLA-SVR-RESP</td>
<td>This protocol anomaly is a Gnutella server response that does not use the expected syntax. Correct syntax for Gnutella 0.4 is: GNUTELLA OK&lt;CR&gt;&lt;LF&gt;; correct syntax for Gnutella 0.6 is: GNUTELLA/0.6 200 OK&lt;CR&gt;&lt;LF&gt;.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:AUDIT:GNUTELLA-TTL</td>
<td>This protocol anomaly is a Gnutella message with a TTL that exceeds the user-defined maximum. The default TTL is 8. The Gnutella RFC recommends an 8 to 10 TTL maximum for Gnutella messages.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:AUDIT:GNUTELLA-UNSUP-VER</td>
<td>This protocol anomaly is a Gnutella message with a connect string that does not conform to Gnutella RFC or the requesting Gnutella version is not 0.4 or 0.6.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:BITTORRENT:TRACKER-QUERY</td>
<td>This signature detects requests to a BitTorrent tracker website. Users may be querying the tracker to look for files to download.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:BITTORRENT:TRACKER-SCRAPE</td>
<td>This signature detects ‘scrape’ requests to a BitTorrent tracker website. Users may be querying the tracker to look for files to download.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:DC:DC-PP-ACTIVE</td>
<td>This signature detects use of the Direct Connect Plus Plus (DC+ + ) file sharing client.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:EDONKEY:CLIENT-VER-CHECK</td>
<td>This signature detects version checks by eDonkey 2000, a peer-to-peer file sharing client. The eDonkey client occasionally checks its own version number to ensure that the client is current.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:GNUTELLA:CONNECT</td>
<td>This signature detects Gnutella client connection requests. Because Gnutella does not use a fixed port number, this signature searches TCP connections to port 1024 and higher by default.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:GNUTELLA:CONNECTION-OK</td>
<td>This signature detects Gnutella server responses to a connection request. Because Gnutella does not use a fixed port number, this signature searches TCP connections to port 1024 and higher by default.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:GNUTELLA:CONNECTION-OK-V06</td>
<td>This signature detects Gnutella server responses to a connection request. Because Gnutella does not use a fixed port number, this signature searches TCP connections to port 1024 and higher by default.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:MLDONKEY:CLIENT-ACTIVE</td>
<td>This signature detects activity by the peer-to-peer (P2P) file sharing client MLDonkey, a multi-protocol P2P file sharing application.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:SKYPE:VERSION-CHECK</td>
<td>This signature detects a Skype client request (to a central server) that checks for the latest version of the client software.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:WINMX:CLIENT-MATCHMAKE-DNS</td>
<td>This signature detects a WinMX client performing DNS lookups for matchmaking servers. WinMX is a peer-to-peer file sharing client that tests firewall rules and reverse-connectivity to determine the most effective way to share files. WinMX queries a matchmaking server to obtain Supernode lists, which enable the WinMX client to share files.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>P2P:WINMX:CLIENT-NET-PRB-DNS</td>
<td>This signature detects a WinMX client performing DNS lookups for hosts that WinMX will probe for connectivity. WinMX is a peer-to-peer file sharing client that tests firewall rules and reverse-connectivity to determine the most effective way to share files.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:WINMX:CLIENT-VER-CHK</td>
<td>This signature detects an initial connection by WinMX, a peer-to-peer file sharing client. WinMX queries a Web site for new versions of the WinMX client software.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>P2P:WINMX:CLIENT-VER-CHK-DNS</td>
<td>This signature detects attempts to obtain the IP address of the host that tracks WinMX client versions. WinMX is a peer-to-peer file sharing client.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:DOS:MDAEMON-POP-DOS</td>
<td>This signature detects denial-of-service attempts against the Mdaemon POP3 Server. Mdaemon v.6.0.7 and earlier versions are vulnerable. Attackers may send a maliciously crafted DELE or UIDL request to the POP3 daemon to crash the POP3, SMTP, and IMAP services.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>POP3:ERROR:BOUNDARY_MISSING</td>
<td>This protocol anomaly is a message with a multipart content type but no boundary.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-386</td>
<td>This signature detects email attachments that have the extension .386 and were received via POP3. Because .386s ( Windows Enhanced Mode Driver) files contain executable code, this may indicate an incoming email virus. Attackers may create malicious executables, tricking users into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-ADE</td>
<td>This signature detects email attachments that have the extension .ade and were received via POP3. Because .ADEs (Microsoft Access Project Extension) files can contain macros, this may indicate an incoming email virus. Attackers may create malicious scripts, tricking users into executing the macros and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-ADP</td>
<td>This signature detects email attachments that have the extension .adp and were received via POP3. Because .ADPs (Microsoft Access Project) files can contain macros, this may indicate an incoming email virus. Attackers may create malicious scripts, tricking users into executing the macros and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-BAS</td>
<td>This signature detects email attachments that have the extension .bas and were received via POP3. Because .BASs (Microsoft Visual Basic Class Module) files contain executable code, this may indicate an incoming email virus. Attackers may create malicious executables, tricking users into executing the file and infecting the system.</td>
<td>low</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-BAT</td>
<td>This signature detects email attachments with the extension '.bat' received via POP3. This may indicate an incoming email virus. .BATS (executable files) contain one or more scripts. Attackers may create malicious executables, tricking the user into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-CHM</td>
<td>This signature detects email attachments that have the extension .chm and were received via POP3. Because .CHMs (Compiled HTML Help File) files can contain scripts, this may indicate an incoming email virus. Attackers may create malicious scripts, tricking users into executing the files and infecting the system.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>POP3:EXT:DOT-CMD</td>
<td>This signature detects email attachments with the extension '.cmd' sent via POP3. This may indicate an incoming email virus. CMD files contain commands that when executed can cause significant damage to a windows system.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-COM</td>
<td>This signature detects email attachments with the extension '.com' received via POP3. This may indicate an incoming email virus. COMs (executable files) contain one or more scripts. Attackers may create malicious executables, tricking the user into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-CPL</td>
<td>This signature detects email attachments with the extension '.cpl' received via POP3. This may indicate an incoming email virus. CPLs (Control Panel elements) are standard Microsoft Windows files that contain Windows Control Panel settings. Attackers may hide malicious executables within a CPL file, tricking users into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-CRT</td>
<td>This signature detects email attachments that have the extension .crt and were received via POP3. Because .CRTs (Security Certificate) files can contain executable code, this may indicate an incoming email virus. Attackers may create malicious executable code, tricking users into executing the file and infecting the system.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-EXE</td>
<td>This signature detects email attachments with the extension '.exe' sent via POP3. This may indicate an incoming email virus. EXEs (Executable files) contain one or more scripts. Attackers may create malicious executables, tricking the user into executing the file and infecting the system.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-GRP</td>
<td>This signature detects GRP files sent over POP3. GRP files can contain Windows Program Group information, and may be exploited by malicious users to deposit instructions or arbitrary code on a target's system. User involvement is required to activate GRP files; typically they are attached to a harmless-appearing e-mail message.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-HLP</td>
<td>This signature detects email attachments that have the extension .hlp and were received via POP3. Because .HLPs (Help File) files can contain macros, this may indicate an incoming email virus. Attackers may create malicious scripts, tricking users into executing the macros and infecting the system.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-HT</td>
<td>This signature detects email attachments with the extension '.ht' sent via POP3. This may indicate an incoming email virus or other attack. HT files contain configuration information for the Hyperterm console program, shipped with every Windows operating system since Windows 95. It is the default handler program for .ht files. A recent vulnerability in Hyperterm could allow an attacker to take control of your computer via an infected .ht file. These files are not normally sent via email.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-HTA</td>
<td>This signature detects email attachments with the extension .hta received using POP3. This may indicate an incoming email virus. HTA files are HTML application files that can be executed by a web browser. Generally, HTA files are not sent via email. As a general network security precaution, ensure that all users are aware of the dangers of sending and receiving binary files in email attachments.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>POP3:EXT:DOT-INF</td>
<td>This signature detects email attachments that have the extension .inf and were received via POP3. Because .INFs (Setup Information) files contain scripts, this may indicate an incoming email virus. Attackers may create malicious scripts, tricking users into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-INS</td>
<td>This signature detects email attachments that have the extension .ins and were received via POP3. Because .INSs (Internet Naming Service) files contain configuration parameters, this may indicate an incoming email virus. Attackers may include malicious configurations, tricking users into executing the file and infecting the system.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-ISP</td>
<td>This signature detects email attachments that have the extension .isp and were received via POP3. Because .ISPs (Internet Communication Settings) files contain configuration parameters, this may indicate an incoming email virus. Attackers may include malicious configurations, tricking users into executing the file and infecting the system.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-JS</td>
<td>This signature detects email attachments that have the extension .ss and were received via POP3. Because .JSs (JavaScript File) files contain scripts, this may indicate an incoming email virus. Attackers may create malicious scripts, tricking users into executing the file and infecting the system.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-JSE</td>
<td>This signature detects email attachments that have the extension .jse and were received via POP3. Because .JSEs (JavaScript Encoded) files contain scripts, this may indicate an incoming email virus. Attackers may create malicious scripts, tricking users into executing the file and infecting the system.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-LNK</td>
<td>This signature detects email attachments that have the extension .lnk and were received via POP3. Because .LNKs (Windows link) files can point to any program, this may indicate an incoming email virus. Attackers may create a link pointing to a dangerous program, tricking users into executing the link and affecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-MDB</td>
<td>This signature detects email attachments that have the extension .mdb and were received via POP3. Because .MDBs (MS Access Application) files can contain scripts, this may indicate an incoming email virus. Attackers may create malicious scripts, tricking users into executing the file and infecting the system.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-MDE</td>
<td>This signature detects email attachments that have the extension .mde and were received via POP3. Because .MDEs (Microsoft Access MDE database) files can contain scripts and macros, this may indicate an incoming email virus. Attackers may create malicious scripts, tricking users into executing the file and infecting the system.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-MSC</td>
<td>This signature detects email attachments that have the extension .msc and were received via POP3.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>POP3:EXT:DOT-MSI</td>
<td>This signature detects email attachments with the extension .msi received via POP3. This may indicate an incoming email virus. .MSIs (Microsoft Windows Installer Package) contain executable code. Attackers may create malicious executables, tricking the user into executing the file and infecting the system.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-MSP</td>
<td>This signature detects email attachments with the extension .msp received via POP3. This may indicate an incoming email virus. .MSPs (Microsoft Windows Installer Patch) contain executable code. Attackers may create malicious executables, tricking the user into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-OCX</td>
<td>This signature detects email attachments that have the extension .ocx and were received via POP3. Because .OCXs (Object Control Extension) files can contain multiple scripts, this may indicate an incoming email virus. Attackers may create malicious executables, tricking users into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-PCD</td>
<td>This signature detects email attachments that have the extension . received via POP3. Because .PCDs (Photo CD MS Compiled Script) files can contain scripts, this may indicate an incoming email virus. Attackers may create malicious scripts, tricking users into executing the file and infecting the system.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-PIF</td>
<td>This signature detects email attachments with the extension .pif sent via POP3. This may indicate an incoming email virus. PIFs (Program Information Files) are standard Microsoft Windows files that contain start up properties for DOS applications. Attackers may hide malicious executables within a PIF file, tricking users into executing the file and infecting the system.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-REG</td>
<td>This signature detects email attachments that have the extension .reg and were received via POP3. Because .REGs (Registry Entries) files contain entries for the Registry, this may indicate an incoming email virus. Attackers may create malicious entries, tricking users into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-SCR</td>
<td>This signature detects email attachments with the extension .scr sent via POP3. This may indicate an incoming email virus. SCRs (ScreenSaver files) are renamed '.exe' files containing executable code. Attackers may disguise malicious executables to appear as harmless screensaver files, tricking the user into executing the file and infecting the system.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-SCT</td>
<td>This signature detects email attachments with the extension .sct received via POP3. This may indicate an incoming email virus. .SCTs (Windows Script Component) contain scripts. Attackers may create malicious scripts, tricking the user into executing the file and infecting the system.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT-URL</td>
<td>This signature detects email attachments with the extension .url received via POP3. This may indicate an incoming email virus. .URLs (Internet Shortcut) contain a link to a web location. Attackers may create a malicious shortcut, tricking the user into executing the file and send the user to a malicious website.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>POP3:EXT:DOT:VB</td>
<td>This signature detects email attachments with the extension .vb received via POP3. This may indicate an incoming email virus. VBs (VBScript File) contain scripts. Attackers may create malicious scripts, tricking the user into executing the file and infecting the system.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT:VBE</td>
<td>This signature detects email attachments with the extension .vbe received via POP3. This may indicate an incoming email virus. VBEs (VBScript Encoded Script File) contain scripts. Attackers may create malicious scripts, tricking the user into executing the file and infecting the system.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT:VBS</td>
<td>This signature detects email attachments with the extension '.vbs' sent via POP3. This may indicate an incoming email virus. VBs (Visual Basic files) contain one or more executable scripts. Attackers may create malicious VB files, tricking the user into executing the file and infecting the system.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT:WMF</td>
<td>This signature detects Metafiles files sent over POP. Windows Metafiles and Enhanced Metafiles files can exploit a Windows GDI vulnerability and may be exploited by malicious users to deposit instructions or arbitrary code on a target's system. User involvement is required to activate Metafiles; typically they are attached to a harmless-appearing e-mail message.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT:WSC</td>
<td>This signature detects email attachments with the extension .wsc received via POP3. This may indicate an incoming email virus. WSCs (Windows Script Component) contain scripts. Attackers may create malicious scripts, tricking the user into executing the file and infecting the system.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT:WSF</td>
<td>This signature detects email attachments with the extension .wsf received via POP3. This may indicate an incoming email virus. WSFs (Windows Script File) contain scripts. Attackers may create malicious scripts, tricking the user into executing the file and infecting the system.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT:WSH</td>
<td>This signature detects email attachments with the extension .wsh received via POP3. This may indicate an incoming email virus. WSHs (Windows Script Host Settings File) contain configuration parameters. Attackers may create malicious configurations, tricking the user into executing the file and infecting the system.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOT:ZIP</td>
<td>This signature detects email attachments with the extension .zip received using POP3. This may indicate an incoming email virus. Zip files are compressed files that can contain one or more executables. Attackers may compress malicious executables within a .zip file, tricking unsuspecting users into executing the file and infecting the system. Because Zip files are frequently used for non-malicious purposes, this signature can generate false positives. As a general network security precaution, ensure that all users are aware of the dangers of sending and receiving binary files in email attachments.</td>
<td>low</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:EXT:DOUBLE-DOT-DOT</td>
<td>This signature detects email attachments that contain two file extensions. Attackers or viruses may send email attachments that use two file extensions to disguise the actual file name and trick users into opening a malicious attachment.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>--------------</td>
</tr>
<tr>
<td>POP3:FAILURE:BRUTE-FORCE</td>
<td>This protocol anomaly is multiple login failures within a short period of time between a unique pair of hosts. The default is 4.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:OUTLOOK:TROUBLE-QUERY-OF</td>
<td>This signature detects buffer overflow attempts against an ActiveX control in Microsoft Outlook. The Local Troubleshooter ActiveX control has inadequate bounds for checking its Query function, and this exploit bypasses normal Outlook/IE ActiveX security controls. Attackers may create a malicious Web site that contains a call to this ActiveX control; this call contains an overly long string that overflows the control buffer, enabling the attacker to gain control of the target system with the user privileges.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:OVERFLOW:APOP</td>
<td>This protocol anomaly is a POP3 APOP command argument that is too long. This may indicate a buffer overflow attempt.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>POP3:OVERFLOW:BOUNDARY_OVERFLOW</td>
<td>This protocol anomaly is a message with more than 70 boundary characters.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:OVERFLOW:COMMAND</td>
<td>This protocol anomaly is a POP3 command that exceeds 4 bytes, the standard length for a POP3 command. This may indicate a non-standard POP3 client/server or an attacker has gained command-line access to the server.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>POP3:OVERFLOW:CONTENT_NAME</td>
<td>This protocol anomaly is a mime header content-type with a name length that is longer than the defined value. The default value is 128.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:OVERFLOW:FILENAME2LONG</td>
<td>This protocol anomaly is a message with a content_disposition header containing a 'name' attribute value that is too long.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:OVERFLOW:LINE</td>
<td>This protocol anomaly is a text-line from a POP3 client to the server that is too long. This may indicate a buffer overflow attempt.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>POP3:OVERFLOW:PASS</td>
<td>This protocol anomaly is a POP3 PASS command argument that is too long. This may indicate a buffer overflow attempt.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>POP3:OVERFLOW:QPOP-OF1</td>
<td>This signature detects buffer overflow attempts against Qpopper, a POP3 server for Unix. Qpopper 3.0beta20 and earlier versions are vulnerable.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>POP3:OVERFLOW:QPOP-OF2</td>
<td>This signature detects a buffer overflow attempt to exploit a vulnerability in Qpopper. Version 3.0beta30 and many earlier versions are vulnerable.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>POP3:OVERFLOW:QPOP-OF3</td>
<td>This signature detects buffer overflow attempts to exploit a vulnerability in the Qpopper daemon. Some 3.0 beta versions are vulnerable.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>POP3:OVERFLOW:QPOP-OF4</td>
<td>This signature detects a buffer overflow attempt to exploit a vulnerability in Qpopper using custom shellcode. Version 3.0beta20 and many earlier versions are vulnerable.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>POP3:OVERFLOW:TXTLINE_2LONG</td>
<td>This protocol anomaly is a message data line that exceeds the defined maximum length (sc_mime_textline_length).</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:OVERFLOW:USER</td>
<td>This protocol anomaly is a POP3 USER command argument that is too long. This may indicate a buffer overflow attempt.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>------------</td>
</tr>
<tr>
<td>POP3:REQERR:REQ-MESSAGE-NUMBER</td>
<td>This protocol anomaly is a POP3 message number that is unreasonably high. This may indicate a huge mailbox or an exploit attempt.</td>
<td>high</td>
<td>sos5.0.0,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>POP3:REQERR:REQ-SYNTAX-ERROR</td>
<td>This protocol anomaly is an unparsed POP command line or header line. This may indicate a non-standard email client or server or a backdoor/exploit attempt.</td>
<td>medium</td>
<td>sos5.0.0,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SCAN:AMAP:FTP-ON-HTTP</td>
<td>This signature detects the scanner tool amap, made by the Hacker's Choice. THC-AMAP is used in initial reconnaissance for an attacker to determine services running on target hosts before launching other attacks.</td>
<td>low</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SCAN:AMAP:SAP-R3-ON-HTTP</td>
<td>This signature detects the scanner tool AMAP, made by The Hacker's Choice (THC). Attackers may use THC-AMAP during their initial reconnaissance to determine services running on target hosts before launching other attacks.</td>
<td>low</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SCAN:AMAP:SSL-ON-HTTP</td>
<td>This signature detects the scanner tool AMAP, made by The Hacker's Choice (THC). Attackers may use THC-AMAP during their initial reconnaissance to determine services running on target hosts before launching other attacks.</td>
<td>low</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SCAN:AMAP:SSL-ON-POP3</td>
<td>This signature detects the scanner tool AMAP, made by The Hacker's Choice (THC). Attackers may use THC-AMAP during their initial reconnaissance to determine services running on target hosts before launching other attacks.</td>
<td>low</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SCAN:METASPLOIT:SMB-ACTIVE</td>
<td>This signature detects traffic generated by the open-source exploiting tool Metasploit Framework. Other signatures may also trip. This indicates that someone is using this tool on your network. Follow-up investigation of source or target machines may be required.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SCAN:MISC:HTTP:HTR-OVERFLOW</td>
<td>&quot;This signature detects denial-of-service (DoS) attacks against Microsoft IIS 4.0 and 5.0. Attackers may send maliciously crafted HTR requests (.htr) with long variable names to overflow the buffer in the ism.dll ISAPI extension that implements HTR scripting and create a denial of service or execute arbitrary commands.&quot;</td>
<td>medium</td>
<td>sos5.0.0,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SHELLCODE:AIX:NOOP-PKT</td>
<td>This signature scans PACKETS for at least four in a raw AIX NOOP instructions, which are very common in buffer overflow exploits. You may want to apply this signature to all non-TCP traffic to your AIX servers.</td>
<td>medium</td>
<td>sos5.0.0,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SHELLCODE:BSDX86:GEN-1-PKT</td>
<td>This signature scans PACKETS for an x86 BSD (all flavors) instruction sequence, common in buffer overflow exploits. You may want to apply this signature to all non-TCP traffic to your BSD servers.</td>
<td>high</td>
<td>sos5.0.0,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SHELLCODE:BSDX86:GEN-2-PKT</td>
<td>This signature scans PACKETS for an x86 BSD (all flavors) instruction sequence, common in buffer overflow exploits. You may want to apply this signature to all non-TCP traffic to your BSD servers.</td>
<td>high</td>
<td>sos5.0.0,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SHELLCODE:DIGITAL:NOOP-PKT</td>
<td>This signature scans PACKETS for at least four in a row DEC ALPHA NOOP instructions, which are very common in buffer overflow exploits. You may want to apply this signature to all non-TCP traffic to your DEC ALPHA servers.</td>
<td>medium</td>
<td>sos5.0.0,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SHELLCODE:HP-UX:HP-NOOP-1-PKT</td>
<td>This signature scans PACKETS for a HP-UX PA-RISC instruction sequence, common in buffer overflow exploits. You may want to apply this signature to all non-TCP traffic to your HP-UX servers.</td>
<td>medium</td>
<td>sos5.0.0,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>------------</td>
</tr>
<tr>
<td>SHELLCODE:HP-UX:HP-NOOP-2-PKT</td>
<td>This signature scans PACKETS for a HP-UX PA-RISC instruction sequence, common in buffer overflow exploits. You may want to apply this signature to all non-TCP traffic to your HP-UX servers.</td>
<td>medium</td>
<td>sos5.0.0,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMB:AUDIT:INV-PROTOCOL</td>
<td>This protocol anomaly is an invalid SMB protocol. The first four bytes of valid SMB messages are 0xff, 'S', 'M', 'B'. This may be a misbehaving client or an attempt to tunnel through the NETBIOS port.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMB:CONNECT-FROM-LOCALHOST</td>
<td>This signature detects attempts to remotely connect to SMB shares with the NetBIOS hostname of Localhost. Because Localhost logins are not typically performed over the network, this may indicate that an attacker is trying to bypass host-based access controls.</td>
<td>low</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMB:ENUM:NAME-LOOKUP</td>
<td>This protocol anomaly is the <code>pipe\lsarpc</code> (Local Security Authority) named pipe transaction used to execute the LookupAccountName function. Programs such as user2sid and Hyena use this named pipe transaction to validate usernames on the target host.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMB:ERROR:GRIND</td>
<td>This protocol anomaly is multiple login/authentication failures between a unique pair of hosts within a short period of time. Vulnerability scanners and programs like enum that perform dictionary based or password-guessing attacks will likely trigger this attack.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMB:ERROR:INV-MSG-LEN</td>
<td>This protocol anomaly is an invalid session message length in an SMB message.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMB:ERROR:MAL-MSG</td>
<td>This protocol anomaly is a malformed SMB message in which the wcount field is larger than the message size.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMB:EXPLOIT:ACCOUNT-NAME-OF</td>
<td>This signature detects attempts to overflow the SMB Account Name. ISS BlackICE, Proventia, and RealSecure products are vulnerable to this buffer overflow. A successful attack could give an attacker complete control of these systems.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMB:EXPLOIT:DOT-JOB</td>
<td>This signature detects a Microsoft Task Scheduler (.job) file being copied over an SMB network share. Microsoft Windows XP Service Pack 1 and Microsoft Windows 2000 Service Pack 2 and earlier are vulnerable. Attackers may open a malicious .job file in Task Scheduler to execute arbitrary code and compromise the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMB:EXPLOIT:LANMAN-NUKE</td>
<td>This protocol anomaly is a LANMAN request (NetServerEnum, NetServerEnum2, or NetShareEnum) over a named pipe transaction where the max-param-count and/or the max-data-count of the Transaction header is zero. Attackers can use this malformed request to crash an unpatched Microsoft NT, 2000, or XP server.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMB:EXPLOIT:LINUX-TRANS2-OF</td>
<td>This signature detects attempts to exploit a vulnerability in the Server Message Block File System (SMBFS) implemented in the Linux kernel. Kernels 2.4 and 2.6 are vulnerable. Attackers may gain root access on the target host.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMB:EXPLOIT:NULL-Filename</td>
<td>This protocol anomaly is an empty Filename field in the Delete, Rename, Move or Copy SMBs.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMB:EXPLOIT:NULL-PATH</td>
<td>This protocol anomaly is an empty Path field in the Tree Connect SMB. This may be a misbehaving client or an attempt to exploit vulnerabilities in the SMB server.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>SMB:EXPLOIT:NULL-SERVICE</td>
<td>This protocol anomaly is an empty Service field in the Tree Connect SMB. This may be a misbehaving client or an attempt to exploit vulnerabilities in the SMB server.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMB:EXPLOIT:REGISTRY-DOS</td>
<td>DI has detected a suspiciously large registry key in the OpenKey function executed using a named-pipe transaction. Large key sizes in the OpenKey function can cause the winlogon.exe process in Window NT 4.0 to crash.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMB:EXPLOIT:SAMBA-DIR-TRAV</td>
<td>This signature detects SMB requests for pathnames that attempt to traverse the server root. Samba 3.0.5 and earlier versions are vulnerable. Malicious users can send &quot;get&quot;, &quot;put&quot;, and &quot;dir&quot; commands to a Samba server to access files outside the shared directories.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMB:EXPLOIT:WINBLAST-DOS</td>
<td>Microsoft Windows Samba File Sharing Resource Exhaustion Vulnerability</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMB:NETBIOS:INV-CDNAME-ENC</td>
<td>This protocol anomaly is an invalid calling name encoding in the NETBIOS header that encapsulates an SMB. NETBIOS names are 16 bytes and may encode to a maximum of 34 bytes.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMB:NETBIOS:INV-CDNAME-LEN</td>
<td>This protocol anomaly is an invalid called name length in the NETBIOS header that encapsulates an SMB. NETBIOS names are 16 bytes and may encode to a maximum of 34 bytes.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMB:NETBIOS:INV-CGNAME-ENC</td>
<td>This protocol anomaly is an invalid calling name encoding in the NETBIOS header that encapsulates an SMB. NETBIOS names are 16 bytes and may encode to a maximum of 34 bytes.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMB:NETBIOS:INV-CGNAME-LEN</td>
<td>This protocol anomaly is an invalid called name length in the NETBIOS header that encapsulates an SMB. NETBIOS names are 16 bytes and may encode to a maximum of 34 bytes.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMB:NETBIOS:INV-SHDR-LEN</td>
<td>This protocol anomaly is an invalid session header length in the NETBIOS header that encapsulates an SMB. The minimum length of an SMB message is 33 bytes.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMB:NETBIOS:INV-SNAME-LEN</td>
<td>This protocol anomaly is an invalid session name length in the NETBIOS header that encapsulates an SMB. NETBIOS names are 16 bytes and may encode to a maximum of 34 bytes.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMB:NETBIOS:RMT-REG-ACCESS</td>
<td>This signature detects attempts to remotely access the Windows registry. Attackers may use a malicious client to view or modify the contents of the Windows registry.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMB:NETBIOS:SHARE-LVL-SEC</td>
<td>This protocol anomaly is an SMB session with share-level security. A user may gain access to various resources on the server without username or password authentication.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMB:TOOLS:PSEEXEC</td>
<td>This signature detects attempts to upload psexec.exe, an SMB tool for uploading and executing programs interactively. This signature also indicates that the psexec.exe has already logged into the system; Psexec.exe can upload itself to the host only after successful login. Worms often use psexec.exe to propagate.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:AUDIT:REQ-INVALID-CMD-SEQ</td>
<td>This protocol anomaly is an invalid sequence of SMTP commands, which would normally not be issued by an SMTP client or server. This may indicate an attacker manually trying to exploit an SMTP server</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------------</td>
</tr>
<tr>
<td>SMTP:AUDIT:TEXT-LINE</td>
<td>This protocol anomaly is a text line (in the data section) in an SMTP connection that is too long. This may indicate a buffer overflow attempt.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:COMMAND:EXPN</td>
<td>This protocol anomaly is an attempt to use the EXPN command. This command is not used by most standard clients and servers and may reveal information about email accounts.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>SMTP:COMMAND:TURN</td>
<td>This protocol anomaly is an attempt to use the TURN command that exchanges the roles of the email client and server. You may want to ban this command and drop the connection, or edit the SMTP attack objects and change their direction to 'BOTH.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:COMMAND:VRFY</td>
<td>This protocol anomaly is an attempt to use the SMTP VRFY command. This command is not used by most standard clients and servers and may reveal sensitive information about email accounts.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>SMTP:COMMAND:WIZ</td>
<td>This signature detects attempts to determine if the SMTP server supports the &quot;WIZ&quot; command, which may provide anonymous root access.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EMAIL:EUDORA-SPOOF3</td>
<td>This signature detects attempts to spoof an email attachment. Eudora Windows versions prior to up to 6.0.3 are vulnerable. Attackers may send a maliciously crafted email with an illegal &quot;Attachment Converted:&quot; line in the message body to spoof attachments, which can lead to remote code execution.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EMAIL:EUDORA-SPOOF4</td>
<td>This signature detects attempts to spoof an email attachment. Eudora Windows 6.2.0.7 and earlier versions are vulnerable. Attackers may send a maliciously crafted email with an illegal &quot;Attachment Converted:&quot; line in the message body to spoof attachments, which can enable remote code execution.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EMAIL:HEADER-FROM-PIPE</td>
<td>This signature detects attempts to send shell commands via an SMTP email message by exploiting the pipe passthrough vulnerability. Attackers may use the invalid &quot;from</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EMAIL:HEADER-TO-PIPE</td>
<td>This signature detects attempts to send shell commands via an SMTP email message by exploiting the pipe passthrough vulnerability. Attackers may use the invalid &quot;to</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EMAIL:MAIL-FROM-PIPE</td>
<td>This signature detects attempts to send shell commands via an SMTP email message by exploiting the pipe passthrough vulnerability. Attackers may use the invalid &quot;mail from</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EMAIL:RCPT-TO-DECODE</td>
<td>This signature detects attempts to send shell commands via an SMTP email message by exploiting the &quot;decode&quot; email alias vulnerability. Attackers may use the invalid &quot;rcpt to decode&quot; as the &quot;rcpt to&quot; email address to cause Sendmail to reroute data to the program uudecode. Attackers may then send uuencoded data to overwrite files or place an arbitrary .rhosts files onto the system.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>---------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>------------</td>
</tr>
<tr>
<td>SMTP:EMAIL:RCPT-TO-PIPE</td>
<td>This signature detects attempts to send shell commands via an SMTP email message by exploiting the pipe passthrough vulnerability. Attackers may use the invalid &quot;rcpt to</td>
<td>medium</td>
<td>sos5.0.0,</td>
</tr>
<tr>
<td></td>
<td>&quot; as the &quot;rcpt to&quot; email address to cause Sendmail to reroute data to another program. Some SMTP servers have been shown to use the &quot;</td>
<td></td>
<td>sos5.1.0</td>
</tr>
<tr>
<td></td>
<td>&quot; character legitimately.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMTP:EMAIL:REPLY-TO-PIPE</td>
<td>This signature detects attempts to send shell commands via an SMTP email message by exploiting the pipe passthrough vulnerability. Attackers may use the invalid &quot;reply to</td>
<td>medium</td>
<td>sos5.0.0,</td>
</tr>
<tr>
<td></td>
<td>&quot; as the &quot;reply to&quot; email address to cause Sendmail to reroute data to another program. This may also be legitimate traffic from several types of SMTP servers.</td>
<td></td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXCHANGE:DOS</td>
<td>This signature detects denial-of-service (DoS) attempts that exploit a MIME header vulnerability in Microsoft Exchange Server 5.5. Attackers may send an email message with an empty charset value (&quot;&quot;) in the MIME header to cause a denial-of-service (DoS).</td>
<td>high</td>
<td>sos5.0.0,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXCHANGE:INV_BDAT_CMD</td>
<td>This protocol anomaly is a BDAT command that is not chunk-size.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXCHANGE:INV_BDAT_SEC_LEN</td>
<td>This protocol anomaly is a BDAT with a chunk-size larger than 0xffffffff.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXCHANGE:MAL-VERB-XEXCH50</td>
<td>This signature detects attempts to exploit a vulnerability in Microsoft Exchange Server 5.5 and 2000. The command verb &quot;Xexch50&quot;, which is valid only for communication between validated Exchange servers, is handled incorrectly. Attackers may send the command verb with a negative number or a very large positive number to crash the Exchange server, and, in extreme cases with Exchange Server 2000, may also take control of the server.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXPLOIT:EUDORA-URL-SPOOF</td>
<td>This signature detects attempts to exploit a vulnerability in the Eudora mail client. By supplying a link containing character entities, an attacker can force Eudora to display a link as something other than what it really is.</td>
<td>low</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXPLOIT:HCP-QUOTE-SCRIPT</td>
<td>This signature detects attempts to exploit a vulnerability in URL handling with the Microsoft Help and Support Center (HSC) when invoked with an hcp:// URL. By embedding a quote (&quot;) character in the URL, HSC can be instructed to load an arbitrary local file or remote web page, which can then be used to execute scripts in the local zone.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXPLOIT:MIME-TOOLS-EVADE</td>
<td>This signature detects attempts to evade antivirus tools such as MIME Tools, a Linux-based email MIME scanner. The MIME RFC allows for an empty boundary, but most all mail clients use one, while many viruses will not.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-386</td>
<td>This signature detects email attachments that have the extension .386 and were sent via SMTP. Because .386s (Windows Enhanced Mode Driver) files can contain executable code, this may indicate an incoming email virus. Attackers may create malicious executables, tricking users into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-ADE</td>
<td>This signature detects email attachments that have the extension .ade and were sent via SMTP. Because .ADEs (Microsoft Access Project Extension) files can contain macros, this may indicate an incoming email virus. Attackers may create malicious scripts, tricking users into executing the macros and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
</tbody>
</table>
Deep Inspection Alarm Log Entries

<table>
<thead>
<tr>
<th>Attack Name</th>
<th>Attack Description</th>
<th>Severity</th>
<th>Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP:EXT:DOT-ADP</td>
<td>This signature detects email attachments that have the extension .adp and were sent via SMTP. Because .ADPs (Microsoft Access Project) files can contain macros, this may indicate an incoming email virus. Attackers may create malicious scripts, tricking users into executing the macros and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-BAS</td>
<td>This signature detects email attachments that have the extension .bas and were sent via SMTP. Because .BASs (Microsoft Visual Basic Class Module) files contain executable code, this may indicate an incoming email virus. Attackers may create malicious executables, tricking users into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-BAT</td>
<td>This signature detects email attachments with the extension '.bat' sent via SMTP. This may indicate an incoming email virus. .BATs (executable files) contain one or more scripts. Attackers may create malicious executables, tricking the user into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-CHM</td>
<td>This signature detects email attachments that have the extension .chm and were sent via SMTP. Because .CHMs (Compiled HTML Help File) files can contain scripts, this may indicate an incoming email virus. Attackers may create malicious scripts, tricking users into executing the files and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-CMD</td>
<td>This signature detects email attachments with the extension '.cmd' sent via SMTP. This may indicate an incoming email virus. .CMD files contain commands that when executed can cause significant damage to a windows system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-COM</td>
<td>This signature detects email attachments with the extension '.com' sent via SMTP. This may indicate an incoming email virus. .COMs (executable files) contain one or more scripts. Attackers may create malicious executables, tricking the user into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-CPL</td>
<td>This signature detects email attachments with the extension '.cpl' sent via SMTP. This may indicate an incoming email virus. CPLs (Control Panel eLements) are standard Microsoft Windows files that contain Windows Control Panel settings. Attackers may hide malicious executables within a CPL file, tricking users into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-CRT</td>
<td>This signature detects email attachments that have the extension .crt and sent received via SMTP. Because .CRTs (Security Certificate) files can contain executable code, this may indicate an incoming email virus. Attackers may create malicious executable code, tricking users into executing the file and infecting the system.</td>
<td>low</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-EXE</td>
<td>This signature detects email attachments with the extension '.exe' sent via SMTP. This may indicate an incoming email virus. .EXEs (executable files) contain one or more scripts. Attackers may create malicious executables, tricking the user into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-GRP</td>
<td>This signature detects GRP files sent over SMTP. GRP files can contain Windows Program Group information, and may be exploited by malicious users to deposit instructions or arbitrary code on a target's system. User involvement is required to activate GRP files; typically they are attached to a harmless-appearing e-mail message.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-HLP</td>
<td>This signature detects email attachments that have the extension '.hlp' and sent received via SMTP. Because .HLPs (Help File) files can contain macros, this may indicate an incoming email virus. Attackers may create malicious scripts, tricking users into executing the macros and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-HT</td>
<td>This signature detects email attachments with the extension '.ht' sent via SMTP. This may indicate an incoming email virus or other attack. HT files contain configuration information for the Hyperterm console program, shipped with every Windows operating system since Windows 95. It is the default handler program for .ht files. A recent vulnerability in Hyperterm could allow an attacker to take control of your computer via an infected .ht file. These files are not normally sent via email.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-INF</td>
<td>This signature detects email attachments that have the extension '.inf' and were sent via SMTP. Because INFs (Setup Information) files contain scripts, this may indicate an incoming email virus. Attackers may create malicious scripts, tricking users into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-INS</td>
<td>This signature detects email attachments that have the extension '.ins' and were sent via SMTP. Because INSs (Internet Naming Service) files contain configuration parameters, this may indicate an incoming email virus. Attackers may include malicious configurations, tricking users into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-ISP</td>
<td>This signature detects email attachments that have the extension '.isp' and were sent via SMTP. Because ISPs (Internet Communication Settings) files contain configuration parameters, this may indicate an incoming email virus. Attackers may include malicious configurations, tricking users into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-JS</td>
<td>This signature detects email attachments that have the extension '.js' and were sent via SMTP. Because JSs (JavaScript File) files contain scripts, this may indicate an incoming email virus. Attackers may create malicious scripts, tricking users into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-JSE</td>
<td>This signature detects email attachments that have the extension '.jse' and were sent via SMTP. Because JSEs (JavaScript Encoded) files contain scripts, this may indicate an incoming email virus. Attackers may create malicious scripts, tricking users into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-LNK</td>
<td>This signature detects email attachments that have the extension .lnk and were sent via SMTP. Because .LNKs (Windows link) files can point to any program, this may indicate an incoming email virus. Attackers may create a link pointing to a dangerous program, tricking users into executing the link and affecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-MDB</td>
<td>This signature detects email attachments that have the extension .mdb and were sent via SMTP. Because .MDBs (MS Access Application) files can contain scripts, this may indicate an incoming email virus. Attackers may create malicious scripts, tricking users into executing the file and infecting the system.</td>
<td>low</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-MDE</td>
<td>This signature detects email attachments that have the extension .mde and were sent via SMTP. Because .MDEs (Microsoft Access MDE database) files can contain scripts and macros, this may indicate an incoming email virus. Attackers may create malicious scripts, tricking users into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-MSC</td>
<td>This signature detects email attachments that have the extension .msc and were sent via SMTP. Because .MSCs (Microsoft Common Console Document) files can contain configuration information, this may indicate an incoming email virus. Attackers may change the configuration to point to a dangerous command, tricking users into executing the files and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-MSI</td>
<td>This signature detects email attachments with the extension .msi sent via SMTP. This may indicate an incoming email virus. .MSIs (Microsoft Windows Installer Package) contain executable code. Attackers may create malicious executables, tricking the user into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-MSP</td>
<td>This signature detects email attachments with the extension .msp sent via SMTP. This may indicate an incoming email virus. .MSPs (Microsoft Windows Installer Patch) contain executable code. Attackers may create malicious executables, tricking the user into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-OCX</td>
<td>This signature detects email attachments that have the extension .ocx and were sent via SMTP. Because .OCXs (Object Control Extension) files can contain multiple scripts, this may indicate an incoming email virus. Attackers may create malicious executables, tricking users into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-PCD</td>
<td>This signature detects email attachments that have the extension .pcd and were sent via SMTP. Because .PCDs (Photo CD MS Compiled Script) files can contain scripts, this may indicate an incoming email virus. Attackers may create malicious scripts, tricking users into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXT:DOT-PIF</td>
<td>This signature detects email attachments with the extension '.pif' sent via SMTP. This may indicate an incoming email virus. PIFs (Program Information Files) are standard Microsoft Windows files that contain start up properties for DOS applications. Attackers may hide malicious executables within a PIF file, tricking users into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>SMTP::EXT::DOT-REG</td>
<td>This signature detects email attachments that have the extension .reg and were sent via SMTP. Because .REGs (Registry Entries) files contain entries for the Registry, this may indicate an incoming email virus. Attackers may create malicious entries, tricking users into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP::EXT::DOT-SCR</td>
<td>This signature detects email attachments with the extension '.scr' sent via SMTP. This may indicate an incoming email virus. SCRs (ScreenSaver files) are renamed '.exe' files containing executable code. Attackers may disguise malicious executables to appear as harmless screensaver files, tricking the user into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP::EXT::DOT-SCT</td>
<td>This signature detects email attachments with the extension .sct sent via SMTP. This may indicate an incoming email virus. .SCTs (Windows Script Component) contain scripts. Attackers may create malicious scripts, tricking the user into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP::EXT::DOT-URL</td>
<td>This signature detects email attachments with the extension .url sent via SMTP. This may indicate an incoming email virus. .URLs (Internet Shortcut) contain a link to a web location. Attackers may create a malicious shortcut, tricking the user into executing the file and send the user to a malicious website.</td>
<td>low</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP::EXT::DOT-VB</td>
<td>This signature detects email attachments with the extension .vb sent via SMTP. This may indicate an incoming email virus. .VBs (VBScript File) contain scripts. Attackers may create malicious scripts, tricking the user into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP::EXT::DOT-VBS</td>
<td>This signature detects email attachments with the extension '.vbs' sent via SMTP. This may indicate an incoming email virus. VBSs (Visual Basic files) contain one or more executable scripts. Attackers may create malicious VB files, tricking the user into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP::EXT::DOT-WMF</td>
<td>This signature detects metafiles (files with .emf or .wmf extensions) in an email attachment. Some versions of Microsoft Windows produce boundary errors when processing metafiles, enabling attackers to create a denial of service (DoS) and execute arbitrary code.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP::EXT::DOT-WSC</td>
<td>This signature detects email attachments with the extension .wsc sent via SMTP. This may indicate an incoming email virus. .WSCs (Windows Script Component) contain scripts. Attackers may create malicious scripts, tricking the user into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP::EXT::DOT-WSF</td>
<td>This signature detects email attachments with the extension .wsf sent via SMTP. This may indicate an incoming email virus. .WSFs (Windows Script File) contain scripts. Attackers may create malicious scripts, tricking the user into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>-----------</td>
</tr>
<tr>
<td>SMTP:EXT:DOT:WSH</td>
<td>This signature detects email attachments with the extension .wsh sent via SMTP. This may indicate an incoming email virus. WSHs (Windows Script Host Settings File) contain configuration parameters. Attackers may create malicious configurations, tricking the user into executing the file and infecting the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:EXT:JOB</td>
<td>This signature detects an attached Microsoft Task Scheduler (.job) file. Opening a malicious .job file in Task Scheduler may allow for arbitrary code execution, leading to system compromise. This vulnerability is present in Microsoft Windows 2000 Service Pack 2 and later. It is also present in Microsoft Windows XP Service Pack 1.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:IIS:IIS:ENCAPS-RELAY</td>
<td>This signature detects attempts to exploit a vulnerability in the Microsoft SMTP Service in Microsoft IIS. Versions 4.0 and 5.0 are vulnerable. A maliciously crafted 'rcpt to:' command can circumvent email relaying rules. Attackers may impersonate trusted emails or send spam anonymously.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>SMTP:INVALID:2MANY-BOUNDARY</td>
<td>This protocol anomaly is an SMTP boundary depth that exceeds the user-defined maximum. The boundary depth indicates the number of nested attachments in a MIME multipart message. The default boundary depth is 4.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:INVALID:BASE64-CHAR</td>
<td>This protocol anomaly is an SMTP message with base64 encoding that contains an invalid character.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:INVALID:BOUNDARY-MISS</td>
<td>This protocol anomaly is an SMTP message with a content-type multipart that has no boundary parameter. The boundary parameter specifies a text string that is used to delimit the parts of the multipart message.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:INVALID:DUP_AUTH</td>
<td>This protocol anomaly is multiple AUTH commands within a single SMTP transaction.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:INVALID:DUP-BOUNDARY</td>
<td>This protocol anomaly is an SMTP message with a MIME multipart content-type that uses duplicate boundaries.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:INVALID:UNFIN-MULTIPART</td>
<td>This protocol anomaly is an SMTP message with a MIME multipart boundary that exceeds actual multipart data (all data is processed but unfinished boundary delimiters exist).</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:MAJORDOMO:COMMAND-EXEC</td>
<td>This signature detects attempts to send shell commands via an SMTP email message by exploiting the back-tick (') vulnerability in Great Circle Associates Majordomo, a perl-based Internet email list server. When processing a list command, Majordomo compares the &quot;reply to&quot; email address against the advertise/noadvertise lists (if configured). During this comparison, Majordomo may be tricked into executing commands when it expands the back-tick operator (used by UNIX to enclose executable commands in a shell command line). Attackers may use the back-tick operator in the &quot;reply to&quot; email header to execute arbitrary commands on the server.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>SMTP:MAL:ACROBAT:UUEXEC</td>
<td>This signature detects a maliciously crafted PDF file attached to an email. Attackers may insert certain shell metacharacters at the beginning of a uuencoded PDF file to force Adobe Acrobat to execute arbitrary commands upon loading the file.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>SMTP:MAIL:EMAIL-URL-HIDING-ENC</td>
<td>This signature detects attempts to exploit a vulnerability in Microsoft Outlook Express. Attackers may embed binary control characters in a URL that is included in an email; when the URL is viewed, these control characters prevent Outlook Express and Internet Explorer from displaying the complete URL, which may have malicious content.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:MAIL:NOTES-BIGMAIL</td>
<td>This signature detects large email messages (&gt; 12 MB) sent to Lotus Domino servers via a commonly published exploit. Attackers may cause Lotus Domino to exhaust all system memory and cause the service to stop responding.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:MAIL:OUTLOOK-MAILTO-QUOT</td>
<td>This signature detects attempts to exploit a vulnerability in the Outlook 2002 mail client. Attackers may use mailto: URLs that contain &amp;quot; strings to execute arbitrary script commands, enabling them to execute code remotely.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:MAIL:SQM-CONTENT-XSS</td>
<td>This signature detects attempts to exploit a vulnerability in SquirrelMail, a PHP4 Webmail package. Attackers may send email messages that contain Javascript in the Content-Type field; when SquirrelMail receives the message, it may interpret and execute the Javascript, enabling the attacker to compromise the target system.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>SMTP:MDAEMON:SEND-OF</td>
<td>This signature detects buffer overflow attempts against the MDaemon mail server. MDaemon 6.7.9 and older versions are vulnerable. Attackers may send an overly long SMTP SAML, SOML, or SEND command to overflow the buffer and crash the MDaemon service; attackers may also obtain complete control of the server with SYSTEM level access.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP: MSSQL-WORM-EMAIL</td>
<td>This signature detects attempts to send an email to <a href="mailto:ixltd@postone.com">ixltd@postone.com</a>. This may indicate the presence of SQLsnake, a MSSQL worm. SQLsnake infects Microsoft SQL Servers that have SA (administrative) accounts without passwords. The worm sends a password list and other system information via email to <a href="mailto:ixltd@postone.com">ixltd@postone.com</a>, then begins scanning for vulnerable hosts listening on TCP/1433.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>SMTP: OVERFLOW:BOUNDARY</td>
<td>This protocol anomaly is an SMTP message with a boundary length that exceeds 70 characters. The SMTP RFC specifies 70 as the maximum number of characters in a boundary.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP: OVERFLOW:COMMAND-LINE</td>
<td>This protocol anomaly is a text line (in the command section, before the DATA command) in an SMTP connection that is too long. This may indicate a buffer overflow attempt.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>SMTP: OVERFLOW:CONTENT-NAME</td>
<td>This protocol anomaly is an SMTP content-type name that exceeds the user-defined maximum. The default number of bytes in a content-type name is 128.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP: OVERFLOW:EMAIL-ADDRESS</td>
<td>This protocol anomaly is an email address that is too long. This may indicate a buffer overflow attempt.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>SMTP: OVERFLOW:EMAIL-DOMAIN</td>
<td>This protocol anomaly is a domain name within an email address (for example, localhost.localdomain in <a href="mailto:root@localhost.localdomain">root@localhost.localdomain</a>) that is too long. This may indicate a buffer overflow attempt.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>SMTP: OVERFLOW:EMAIL-USERNAME</td>
<td>This protocol anomaly is a user name within an email address (for example, root in <a href="mailto:root@localhost.localdomain">root@localhost.localdomain</a>) that is too long. This may indicate a buffer overflow attempt.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>SMTP:OVERFLOW:FILENAME</td>
<td>This protocol anomaly is an SMTP content-disposition filename that exceeds the user-defined maximum. The default number of bytes in a content-disposition filename is 128.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:OVERFLOW:METAMAIL-HDR-FS2</td>
<td>This signature detects SMTP messages with headers that contain format string errors. Metamail 2.7 and earlier versions are vulnerable. Because Metamail does not handle SMTP headers correctly, attackers may send maliciously crafted SMTP messages to execute arbitrary code at the same privilege level as the target (typically a user). Note: Systems that typically carry non-English email messages should not include this attack object in their Security Policy.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:OVERFLOW:METAMAIL-HDR-OF1</td>
<td>This signature detects SMTP messages with large headers that contain character set information. Metamail 2.7 and earlier versions are vulnerable. Because Metamail does not handle SMTP headers correctly, attackers may send maliciously crafted SMTP messages to execute arbitrary code at the same privilege level as the target (typically a user). Note: Systems that typically carry non-English email messages should not include this attack object in their Security Policy.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:OVERFLOW:METAMAIL-HDR-OF2</td>
<td>This signature detects SMTP messages with large headers that contain character set information. Metamail 2.7 and earlier versions are vulnerable. Because Metamail does not handle SMTP headers correctly, attackers may send maliciously crafted SMTP messages to execute arbitrary code at the same privilege level as the target (typically a user). Note: Systems that typically carry non-English email messages should not include this attack object in their Security Policy.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:OVERFLOW:OUTLOOK-CERT-OF</td>
<td>This signature detects buffer overflow attempts against Microsoft Outlook Express, which ships with Internet Explorer 5.5. Attackers may send a maliciously crafted email to a host; if the host opens the email in Outlook Express, attackers may execute arbitrary code on the host.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>SMTP:OVERFLOW:REPLY-LINE</td>
<td>This protocol anomaly is a server reply line in an SMTP connection that is too long. This may indicate a buffer overflow attempt by a compromised or malicious SMTP server.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>SMTP:OVERFLOW:SENDMAIL-CMT-OF1</td>
<td>This signature detects attempts to exploit a vulnerability in Sendmail. Sendmail versions 5.79 to 8.12.7 are vulnerable. Attackers may include multiple empty address containers in an SMTP header field to overflow the SMTP header buffer and force Sendmail to execute arbitrary code on the host; attackers may obtain root access.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>SMTP:OVERFLOW:SENDMAIL-CMT-OF2</td>
<td>This signature detects attempts to exploit a vulnerability in Sendmail. Sendmail versions 5.79 to 8.12.7 are vulnerable. Attackers may include multiple empty address containers in an SMTP header field to overflow the SMTP header buffer and force Sendmail to execute arbitrary code on the host.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>SMTP:OVERFLOW:SENDMAIL-MIME-OF</td>
<td>This signature detects buffer overflow attempts against Sendmail. Sendmail versions 8.8.0 and 8.8.1 are vulnerable. Attackers may embed a maliciously crafted MIME header in an email to overflow a buffer in Sendmail and execute arbitrary commands as root.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-------------</td>
<td>--------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>SMTP:OVERFLOW:SQRLMAIL-HDR-INJ</td>
<td>This signature detects SMTP messages with Base-64 encoded headers. SquirreIMail 1.4.3a and earlier versions do not correctly sanitize SMTP headers. Attackers may send maliciously crafted SMTP messages to execute arbitrary code at the same privilege level as the target (typically user). Note: Systems that typically carry non-English email messages should not include this attack object in their Security Policy.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:OVERFLOW:TOO-MANY-RCPT</td>
<td>This protocol anomaly is too many ‘RCPT TO:’ recipients in an SMTP connection. This may indicate a very popular email message or a DoS/buffer overflow attempt.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>SMTP:REQERR:REQ-SYNTAX-ERROR</td>
<td>This protocol anomaly is an unparsed SMTP command line or header line due to a missing ‘:’. This may indicate a non-standard email client or server or a backdoor/exploit attempt.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:RESPONSE:PIPE-FAILED</td>
<td>This signature detects SMTP server responses that are generated when an unsuccessful attempt is made to send shell commands via an SMTP email message by exploiting the pipe (</td>
<td>) passthrough vulnerability in SendMail. If the '</td>
<td>' operator was used within specified &quot;mail to&quot; and/or &quot;rcpt to&quot; email addresses to cause Sendmail to reroute data to another program, attackers receive a '550' error message.</td>
</tr>
<tr>
<td>SMTP:SAGTUBE-DOS</td>
<td>This signature detects character strings within an email message that are designed to exploit a vulnerability in SpamAssassin. SpamAssassin Project SpamAssassin 2.63 and earlier are vulnerable. SpamAssassin uses a weighting system to determine when an email message is spam. Attackers may send a maliciously crafted email with a spoofed address to cause SpamAssassin to consider all further email from the spoofed address as spam, regardless of the target's whitelist settings. After the malicious email has been received by the target, SpamAssassin blocks all emails from the spoofed address.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>SMTP:SENDMAIL:ADDR-PRESCAN-ATK</td>
<td>This signature detects attempts to exploit a vulnerability in Sendmail SMTP server versions prior to 8.12.9. Because the prescan() procedure that processes email addresses in SMTP headers does not perform some char and int conversions correctly, attackers may send a maliciously crafted request to corrupt the Address Prescan Memory on a Sendmail SMTP server and execute arbitrary code.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>SMTP:SENDMAIL:SENDMAIL-FF-OF</td>
<td>This signature detects attempts to exploit a vulnerability in Sendmail versions 8.12.8 and earlier. Under certain conditions, the Sendmail address parser does not perform sufficient bounds checking when converting char to int. Attackers may use this exploit to gain control of the server.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>TROJAN:AUTOPROXY:INFECTED-HOST</td>
<td>This signature detects the AutoProxy trojan attempting to contact a master server and register the IP address and open ports of the infected host. AutoProxy is a trojan that installs a proxy server on Microsoft Windows hosts. Attackers may use an infected host to attack other targets while masking their actual IP address.</td>
<td>critical</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>TROJAN:MISC:MOONPIE3-FTP-RESP</td>
<td>This signature detects a banner from the FTP server embedded in the MoonPie backdoor version 3.0 (other versions may also be detected).</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>TROJAN:MISC:WANREMOTE-ADMIN</td>
<td>This signature detects access to the WanRemote administration interface using the HTTP protocol.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>TROJAN:MS-04-028:BACKDOOR-LOGIN</td>
<td>This signature detects login attempts from a client infected with a trojan installed as part of the Microsoft GDI+ Library JPEG overflow exploit.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>TROJAN:MS-04-028:TOOL-DOWNLOAD</td>
<td>This signature detects attempts by a specific trojan to download files. The trojan, installed as part of the Microsoft GDI+ Library JPEG Overflow exploit, is attempting to download updated files from a remote host.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>TROJAN:PHATBOT:FTP-CONNECT</td>
<td>This signature detects Phatbot FTP connections. Phatbot, a trojan similar to Agobot but with more functionality, sends spam from an infected host machine.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>TROJAN:QAZ:TCP25-CALLING-HOME</td>
<td>This signature detects the string 'nongmin.cn' within an SMTP header-from field sent from a remote system to local server port 25. This may indicate an attacker is attempting to access the Trojan/Worm QAZ. The QAZ Trojan/Worm, famous for infecting the Microsoft network October 2000, allows attackers to access data and gain control over some functions on remote Microsoft Windows systems.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:POP3:BABYLONIA</td>
<td>This signature detects email attachments with the file name 'x-mas.exe' sent via POP3. This may indicate the Babylonia email virus is attempting to enter the system. The executed virus infects all files greater than 8kb, installs automatic virus updaters, and allows attackers to further compromise the system by uploading trojans, creating backdoors, etc.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:POP3:BADASS</td>
<td>This signature detects email attachments with the file name 'badass.exe' sent via POP3. This may indicate the BadAss email virus is attempting to enter the system. The executed virus displays a message box with specified text, opens the Microsoft Outlook database, and sends infected messages containing a Dutch phrase to all addresses found.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:POP3:EICAR-ATTACHMENT</td>
<td>This signature detects the EICAR antivirus test file sent as an email attachment.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:POP3:EUROCALCULATOR</td>
<td>This signature detects email attachments with the file name 'Eurocalculator.exe' sent via POP3. This may indicate the Eurocalculator Trojan is attempting to enter the system. The executed file installs a remote administration Trojan similar to Back Orifice, allowing attackers to access data and gain control over some functions on remote Microsoft Windows systems.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:POP3:EXPLOREZIP-B</td>
<td>This signature detects email attachments with the file name 'zippati.exe' sent via POP3. This may indicate the email virus ExploreZip.B is attempting to enter the system. The executed.ZIP file (zippati in Italian) installs the program explore.exe, which edits the host and visible networked WIN.INI files to run explore.exe on startup. The virus also searches all local and visible networked drives for common file types (.ASN, .C, .CPP, .DOC, .H, .XLS, .PPT) and reduces them to zero bytes.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>VIRUS:POP3:FI2001</td>
<td>This signature detects email attachments with the file name 'fix2001.exe' sent via POP3. This may indicate the email virus Fix2001 is attempting to enter the system. The executed file edits the Registry to run the virus on startup, obtains email addresses from sent and received messages, and sends infected email messages to all addresses found. If the virus is patched or corrupted, it also overwrites the C:COMMAND.COM file with a denial-of-service (DoS) (DoS) trojan that erases all drive data upon reboot.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:POP3:FREELINK</td>
<td>This signature detects email attachments named 'Link.vbs' sent via POP3. This may indicate the VBS.Freelink email virus is attempting to enter the system. The executed virus edits Microsoft Windows Registry entries, opens the Microsoft Outlook database, and sends infected messages to all addresses found.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:POP3:HAPPY99</td>
<td>This signature detects emails with the header 'X-Spanska: Yes' and the UU-encoded attachment 'Happy99.exe' sent via POP3. This may indicate the email virus/worm Happy99/Ska is attempting to enter the system. The executed file edits files (notably WSOCK32.DLL) in the system directory, obtains email addresses from sent and received messages, and sends infected email messages to all addresses found. Once WSOCK32.DLL is successfully modified, the virus/worm also exhibits a message box animation routine of a fireworks display.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:POP3:IROK</td>
<td>This signature detects email attachments named 'irok.exe' sent via POP3. This may indicate the email virus Irok is attempting to enter the system. The executed file exhibits a message box animation routine of a starfield while copying itself to the Windows system directory and writing the file Irokrun.vbs to the Startup directory. Upon reboot, the VB script uses Windows Scripting Host (WSH) to open the Microsoft Outlook database and send infected files to up to 60 addresses found. This virus also install the file script.ini to the m IRC directory and use dcc to send irok.exe to IRC clients who join the channel.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:POP3:MATRIX</td>
<td>This signature detects emails with the content &quot;Software provided by Matrix&quot; sent via POP3. This may indicate the email virus Matrix is attempting to enter the system. The executed file first checks for antivirus software running on the host and terminates if found. Otherwise, the virus copies itself to the Windows directory as ie.<em>pack.exe, runs, and renames to Win32.dll. Matrix also installs the downloader program Mtx</em>.exe (which downloads plugins for the virus upon reboot), and infects Win32 executables.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:POP3:MYPICS</td>
<td>This signature detects email attachments named 'pics4you.exe' sent via POP3. This may indicate the email virus MyPics is attempting to enter the system. The executed file installs as Pics4You.exe and writes itself to the Windows Startup directory, obtains email addresses from the Microsoft Outlook database, and sends infected email messages to 50 addresses at a time. MyPics was also designed to corrupt CMOS data and reformat hard drives on 1/1/2000.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>--------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>VIRUS:POP3:MYROMEO-BLE-BLA</td>
<td>This signature detects emails with the subject 'ble bla' with the attachments myjuliet.chm and myromeo.exe sent via POP3. This may indicate the email virus Verona is attempting to enter the system. Because CHM files are compressed HTML files, myjuliet.chm is activated when viewed in the Microsoft Outlook preview pane; once triggered, the CHM file runs myromeo.exe in the background. Myromeo.exe obtains email addresses from the Microsoft Outlook database, sends infected email messages to all addresses found, and edits the Window directory file hh.dat.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:POP3:MYROMEO-EXE</td>
<td>This signature detects email attachments with the name 'myromeo.exe' accompanied by myjuliet.chm and sent via POP3. This may indicate the email virus Verona is attempting to enter the system. Because CHM files are compressed HTML files, myjuliet.chm is activated when viewed in the Microsoft Outlook preview pane; once triggered, the CHM file runs myromeo.exe in the background. Myromeo.exe obtains email addresses from the Microsoft Outlook database, sends infected email messages to all addresses found, and edits the Window directory file hh.dat.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:POP3:MYROMEO-I-LOVE-YOU</td>
<td>This signature detects emails with the attachments myjuliet.chm and myromeo.exe sent via POP3. This may indicate the email virus Verona is attempting to enter the system. Because CHM files are compressed HTML files, myjuliet.chm is activated when viewed in the Microsoft Outlook preview pane; once triggered, the CHM file runs myromeo.exe in the background. Myromeo.exe obtains email addresses from the Microsoft Outlook database, sends infected email messages to all addresses found, and edits the Window directory file hh.dat.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:POP3:MYROMEO-MYJULIET</td>
<td>This signature detects email attachments with the name 'myjuliet.chm' accompanied by myromeo.exe and sent via POP3. This may indicate the email virus Verona is attempting to enter the system. Because CHM files are compressed HTML files, myjuliet.chm is activated when viewed in the Microsoft Outlook preview pane; once triggered, the CHM file runs myromeo.exe in the background. Myromeo.exe obtains email addresses from the Microsoft Outlook database, sends infected email messages to all addresses found, and edits the Window directory file hh.dat.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:POP3:NAVIDAD</td>
<td>This signature detects email attachments named 'navidad.exe' sent via POP3. This may indicate the email virus Navidad is attempting to enter the system. The executed file copies itself as winsvrc.vxd to the Windows system directory and edits the Registry to run the virus on reboot, installs into the system tray, and displays a dialog box with the text 'UI.' The virus also intercepts new incoming email addresses and sends infected email messages to all senders.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>VIRUS:POP3:NIMDA</td>
<td>This signature detects email attachments named ‘readme.exe’ sent via POP3. This may indicate the email virus Nimda is attempting to enter the system. The executed file installs to the Windows directory, edits the Registry to run the virus on reboot, and infects Internet-related files. Nimda then obtains email addresses and sends infected messages to all addresses found using its own SMTP server.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:POP3:PAPA</td>
<td>This signature detects email attachments named ‘xpass.xls’ sent via POP3. This may indicate the email virus Papa is attempting to enter the system. The executed Microsoft Excel file obtains email addresses from Microsoft Outlook database and sends infected messages to the first 60 addresses found. Papa also attempts to create a denial-of-service (DoS) by pinging the all.net Web server.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:POP3:PASSION</td>
<td>This signature detects email attachments named ICQ_Greeting.exe sent using POP3. This may indicate the email virus Passion is attempting to enter the system. The executed file copies itself to local root drive, edits the registry to run the virus on reboot, and deletes files. Passion then obtains email addresses from the Microsoft Outlook database and sends infected messages to the first 50 addresses found.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:POP3:PIKACHU-POKEMON</td>
<td>This signature detects emails with the subject ‘Pikachu Pokemon’ sent via POP3. This may indicate the email virus Pikachu Pokemon is attempting to enter the system. The executed file displays a “friendly” message featuring Pikachu while it overwrites the Autoexec.Bat file to delete most Microsoft Windows 9x system files upon reboot. Pikachu then obtains email addresses from Microsoft Outlook database and sends infected messages to all addresses found.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:POP3:PRETTY-PARK</td>
<td>This signature detects emails with the subject ‘C:\CoolProgs\Pretty Park.exe’ sent via POP3. This may indicate the email virus Pretty Park is attempting to enter the system. The executed file copies itself to the Windows System directory as FILES32.VXD and edits the Registry to run the virus on reboot. Pretty Park then obtains email addresses from Microsoft Outlook database and sends infected messages to all addresses found every 30 minutes. The virus also attempts to contact its author via IRC chat every 30 seconds; attackers may use the installed virus as a backdoor remote access tool to further compromise the system.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:POP3:SIMBIOSIS</td>
<td>This signature detects email attachments named ‘SETUP.EXE’ sent via POP3. This may indicate the email virus Simbiosis (Cholera worm executable containing a CTX virus) is attempting to enter the system. The executed Cholera worm copies itself to the Windows directory and edits either the WIN.INI file (Windows 9x) or the Registry (NT) to run the virus on reboot. Simbiosis then obtains email addresses from Internet-related files and sends infected messages to all addresses found using its own SMTP server. The executed CTX virus appends and infects Microsoft Windows PE executables; the virus does not carry a payload and is apparent only through a video effect.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>VIRUS:POP3:SUPPL</td>
<td>This signature detects email attachments named 'Suppl.doc' sent via POP3. This may indicate the email virus/trojan Suppl is attempting to enter the system. The executed file macros copy the active (virus) document to the Windows directory as Anthrax.ini and decompress the malicious Wsock32.dll file appended to Suppl.doc. On reboot, the virus file DLLtmp replaces the malicious Wsock32.dll and the original Wsock32.dll is renamed to Wsock33.dll. Suppl then attaches to all outgoing SMTP email messages, locates files with common extensions (DOC, .TXT, .ZIP, etc) on available hard drives, and truncates those files to zero bytes.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:POP3:THEFLY</td>
<td>This signature detects email attachments named 'The_Fly.chm' sent via POP3. This may indicate the email virus The Fly is attempting to enter the system. The executed file copies itself as THE_FLY.CHM to the Windows directory, as DXGFXB3D.DLL to Windows system directory, and opens a graphic with message 'If you ride a motorcycle, close your mouth'. The Fly then copies MSJSVM.JS to the Windows system directory and edits the Registry to run this JavaScript upon reboot. The virus also obtains email addresses from the Microsoft Outlook database and sends infected messages to all addresses found.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:POP3:TIMOFONICA</td>
<td>This signature detects email attachments named 'Timofonica.txt.vbs' sent via POP3. This may indicate the email virus Timofonica is attempting to enter the system. The executed file creates cmos.com and edits the Registry to run the virus on reboot. When cmos.com is run, it erases CMOS memory, MBRs from the first four physical hard disks, and MBRs and DOS Boot Records of extended partitions. Timofonica also obtains email addresses from the Microsoft Outlook database and sends infected messages to all addresses found. Simultaneously, the virus emails the SMS gateway at Moviestar.net and send SMS messages to random cellular phone numbers.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:POP3:TOADIE</td>
<td>This signature detects email attachments named 'Toadie.exe' sent via POP3. This may indicate the email virus Toadie is attempting to enter the system. The executed file infects EXE files by relocating the initial 7800 bytes to the end of the file, encrypting those bytes, and writing 7800 bytes of its own DOS program to the beginning of the file, thus changing EXE files to DOS files. When run, the virus code first infects more EXE files before passing control. Toadie also replaces unsent email messages in Pegasus Mail, and may send copies of itself via IRC.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>VIRUS:POP3:TRIPLESIX</td>
<td>This signature detects email attachments named '666test.vbs' sent via POP3. This may indicate the email virus TripleSix is attempting to enter the system. The executed file displays three dialogue boxes leading the user through the game &quot;Does your name add up to 666?&quot;. The virus then copies WINTEMP.TXT to the Windows directory; this file creates WINTEMP.EXE (a PkZip executable), which in turn creates 666TEST.ZIP (an archive). The archive is copied to the Windows system directory as WINSWAP.SWP. TripleSix also writes REGSVR.VBS to the Windows system directory and edits the Registry to run that script on reboot. When REGSVR.VBS is activated, it obtains email addresses from the Microsoft Outlook database and sends infected messages to all addresses found, overwrites mIRC and Pirch setup files, and sends infected messages via IRC.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VIRUS:POP3:TUNE</td>
<td>This signature detects email attachments named 'Tune.vbs' sent via POP3. This may indicate the email virus Tune is attempting to enter the system. The executed file copies itself to the Windows, Windows system, and Temporary directories and edits the Registry to run the virus on reboot. When activated, it obtains email addresses from the Microsoft Outlook database and sends infected messages to all addresses found, overwrites mIRC and Pirch setup files, and sends infected messages via IRC.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VIRUS:POP3:UUENCODED-DOT-VBS</td>
<td>This signature detects email attachments containing the string 'begin' and the file extension 'vbs' sent via POP3. This may indicate the email virus LoveLetter is attempting to enter the system. The executed file copies itself to the Windows system directory and edits the Registry to run the virus on reboot; when activated, it downloads a trojan from a specified web site that deletes security keys and sends stolen passwords to its owner. LoveLetter also obtains email addresses from the Microsoft Outlook database and sends infected messages to all addresses found, overwrites mIRC and Pirch setup files, and sends infected messages via IRC.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VIRUS:POP3:WSCRIPT-KAK</td>
<td>This signature detects emails containing 'kak.hta' sent via POP3. This may indicate the email virus Kak is attempting to enter the system. The virus arrives embedded within Microsoft Outlook message signature file as kak.htm, and activates when viewed in the Microsoft Outlook preview pane. Once triggered, the file copies itself as kak.hta to the Windows startup and system directories; on reboot, the virus overwrites the autoexec.bat file to delete the virus from the startup directory. Kak then replaces the Microsoft Outlook message signature with infected file kak.htm. The virus also displays an alert box after 6pm on the first day of the month and shows down Windows.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VIRUS:POP3:Y2K-ZELU</td>
<td>This signature detects email attachments named 'Y2k.exe' sent via POP3. This may indicate the email virus Zelu is attempting to enter the system disguised as the utility ChipTec Y2K Freeware Version. The executed file scans available directories, corrupts writeable files, and inserts a message at the beginning of infected files. Zelu may reset the system, making the operating system unusable and erasing all data.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
</tbody>
</table>

Appendix E: Log Entries
<table>
<thead>
<tr>
<th>Attack Name</th>
<th>Attack Description</th>
<th>Severity</th>
<th>Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>VIRUS:POP3:ZIPPED</td>
<td>This signature detects email attachments named 'ZippedFiles.exe' sent via POP3. This may indicate the email virus Zipped Files is attempting to enter the system. The executed ZIP file installs the program explore.exe, which edits the host and visible networked WIN.INI files to run explore.exe on startup. The virus also searches all local and visible networked drives for common file types (.ASN, .C, .CPP, .DOC, .H, .XLS, .PPT) and reduces them to zero bytes.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:SMTP:BAGLE.Q-SMTP</td>
<td>This signature detects the Q through T variants of the Bagle SMTP virus. Bagle sends emails containing an attachment with a malicious payload. Viewing the email message loads an external link using HTTP; this link is actually an executable program that infects the target. The virus then sends a copy of itself to email addresses found on the target's hard drive using the target's email address as the return address.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:SMTP:DOUBLE-DOT-DOT</td>
<td>This signature detects email attachments that contain two file extensions. Attackers or viruses may send email attachments that use two file extensions to disguise the actual file name and trick users into opening a malicious attachment.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:SMTP:DUMARU.J</td>
<td>This signature detects the J variant of the Dumaru SMTP virus. Dumaru sends emails with the subject line: “Important information for you. Read it immediately!”; the email includes a .zip attachment that contains a malicious payload disguised as a picture. When the picture is viewed, the malicious executable program infects the target host. The virus then sends a copy of itself to email addresses found in the target's address book, using the target's email address as the return address.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:SMTP:ECAR-ATTACHMENT</td>
<td>This signature detects the EICAR antivirus test file sent as an email attachment.</td>
<td>info</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:SMTP:EXE-ATTACH-1</td>
<td>This signature detects Win32 executables sent as a MIME attachment. Many viruses, worms, and other malicious programs are transmitted through SMTP attachments. You might want to block all executable attachments and instead require your users to send executables in a compressed format.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:SMTP:EXE-IN-ZIP</td>
<td>This signature detects Win32 executables sent within a ZIP file as a MIME attachment. Many viruses, worms, and other malicious programs are transmitted through SMTP attachments. You might want to block all executable attachments.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:SMTP:NAIL</td>
<td>This signature detects attempts by the email virus Nail to enter the system. When executed, the virus assigns the Microsoft Word auto.dot template to a template located on an attacker Web site, enabling the attacker to upload new virus code. Nail then starts a MAPI (Mail API) session, obtains email addresses from the Microsoft Outlook database, and sends infected email messages to all addresses found. Finally, the virus sends an email message to <a href="mailto:chainnail@hotmail.com">chainnail@hotmail.com</a>, assumed to be the email address of the virus author.</td>
<td>high</td>
<td>sos5.0.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>VIRUS:SMTP:RESUME-EXPLORER-DOC</td>
<td>This signature detects email attachments named 'EXPLORER.DOC' sent via SMTP. This may indicate the email virus Resume is attempting to enter the system. The executed file obtains email addresses from Microsoft Outlook database and sends infected messages to all addresses found. When the file is closed, Resume creates directory C:Data, copies itself there as Normal.dot, and edits the Registry to run the virus on reboot. The virus then attempts to delete all files from several directories (including Windows) and all drives from A: to Z.</td>
<td>low</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VIRUS:SMTP:SOBIG-ATTACHMENTS</td>
<td>This signature detects email attachments with one of the following file name sent via SMTP: approved.pif, application.pif, doc_details.pif, movie28.pif, password.pif, ref-39xxxx.pif, screen_doc.pif, screen_temp.pif, _approved.pif. This may indicate the SOBIG email virus is attempting to enter the system.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>VOIP:MGMT:XPRESSA-HTTP-DOS</td>
<td>This signature detects attempts to exploit a vulnerability in Pingtel Xpressa phones. Attackers may supply an overly long request to the HTTP management server on the phone to execute arbitrary code or crash the phone (the phone must be rebooted).</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>WORM:AGOBOT:HTTP-SHARE-ENUM</td>
<td>This signature detects attempts by the Agobot worm to enumerate SMB shares via HTTP.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>WORM:AGOBOT:PY-HTTP-PROP</td>
<td>This signature detects the PY variant of the Agobot worm as it attempts to infect another host. This signature could be prone to false positives.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>WORM:BAGLE:AF-HTTP</td>
<td>This signature detects the AF variant of the Bagle SMTP virus. Bagle sends emails that contain an attachment with a malicious payload. When the attachment is viewed, the payload uses HTTP to load an external link, which is actually an executable program that infects the target host. The virus then sends a copy of itself to email addresses found on the target’s hard drive, using the target’s email address as the return address.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>WORM:BAGLE:AF-SMTP</td>
<td>This signature detects the AF variant of the Bagle SMTP virus. Bagle sends emails to victims with an attachment with malicious payload. Attempting to view the attachment, which is actually an executable program, infects the user. The virus then sends a copy of itself to emails found searching the victim’s hard drive for addresses, with the victim’s email address as the return address.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>WORM:BERBEW:KEYLOGGER-UPLOAD</td>
<td>This signature detects the Berbew worm as it uploads keylogger information to a listening post. Berew monitors user keystrokes for financial data and reports that information to an attacker via HTTP to a listening post. Source IP addresses that trigger this signature are extremely likely to be infected with the Berbew worm.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>WORM:BOBAX:C-PHONE-HOME-DNS</td>
<td>This signature detects Bobax worm activity. The C variant of the Bobax worm attempts to lookup the correct IP addresses for listening post servers set up by the Bobax virus authors. Because lookups for these addresses are extremely suspicious, you should investigate the source device for Bobax infection. However, this signature detects Bobax activity (not Bobax infection attempts), and cannot be used to prevent Bobax infection. To prevent Bobax infection, configure your Security Policy to drop traffic that matches the signatures &quot;Windows RPC: LSASS Malicious OpCode&quot; and &quot;Windows RPC: LSASS DCE-RPC Oversized Fragment&quot;.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>WORM:CODERED:INFECTION-ATTEMPT</td>
<td>The signature detects attempts to infect an Microsoft IIS server with the Code Red worm using a .ida buffer-overflow attack. The installed worm downloads code from the donor host, creates a backdoor on the victim, and sets up 100 threads of the worm that scan for other vulnerable hosts using random IP addresses. Code Red also checks the host system time; on the 20th of each month (GMT), all infected systems send 100k bytes of data to TCP/80 of <a href="http://www.whitehouse.gov">www.whitehouse.gov</a>, causing a denial-of-service (DoS).</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>WORM:CODERED-2:CMD-BACKDOOR</td>
<td>This signature detects attempts to access a backdoor web script installed by the Code Red II worm. The Code Red II worm, like the original Code Red worm, allows attackers to remotely access the server.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>WORM:CODERED-2:INFECT-ATTEMPT</td>
<td>This signature detects attempts by the CodeRedII worm to infect a host. The CodeRedII worm, also known as CodeRed.F, exploits the same vulnerability as the original CodeRed worm.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>WORM:CODERED-2:ROOT-BACKDOOR</td>
<td>This signature detects attempts to access a backdoor web script installed by the Code Red II worm. The Code Red II worm, like the original Code Red worm, allows attackers to remotely access the server.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>WORM:EMAIL:BAGLE-INFECTION</td>
<td>This signature detects the Bagle worm activity on a host. After infecting a host, the Bagle worm attempts to contact a Web server listening post. The Bagle worm, which affects Microsoft Windows, copies itself to the system directory, and edits the system registry. The worm uses an email attachment to propagate itself to other hosts, and has a hard-coded expiration date (January 28). This signature could be prone to false positives.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>WORM:EMAIL:W32.SOBIG.E</td>
<td>This signature detects e-mail attachments containing the W32.Sobig.E worm sent via SMTP.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>WORM:MIMAIL:MIMAIL.A</td>
<td>This signature detects the Mimail.A worm attachment in SMTP traffic. After infecting a Windows-based host, Mimail sends itself as an attachment to another target using its own SMTP engine.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>WORM:MIMAIL:MIMAIL.L</td>
<td>This signature detects the Mimail.L worm attachment in SMTP traffic. After infecting a Windows-based host, Mimail sends itself as an attachment to another target using its own SMTP engine.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>Attack Name</td>
<td>Attack Description</td>
<td>Severity</td>
<td>Versions</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>-----------</td>
</tr>
<tr>
<td>WORM:MOFEI:MOFEI-B-PROPAGATION</td>
<td>This signature detects the MoFei worm attempting to propagate to another host. After infecting a host, the MoFei worm propagates by depositing a copy of itself in a vulnerable NetBIOS folder on another host. The MoFei worm is known by several aliases, including W32.Mofei-B and W32.Femot.D.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>WORM:NACHI:B-C-D-INFECT-ATTEMPT</td>
<td>This signature detects infection attempts of the Windows RPC Locator Service by the B, C or D variants of the Nachi worm. This signature only triggers on a successful connect to an accessible victim. Follow up is strongly suggested.</td>
<td>critical</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>WORM:NACHI:D-WEBDAV-ATK</td>
<td>This signature detects WebDAV overflows, which can indicate an infection attempt by the Nachi worm (D variant). Nachi.D, a worm, typically attempts to infect the target host by exploiting several vulnerabilities.</td>
<td>high</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>WORM:NETSKY:V-SMTP-PROP</td>
<td>This signature detects the V variant of the NetSky worm. The V variant encodes a malicious HTML script in the body of an email sent to the target host. Due to a known vulnerability, Microsoft Outlook and Outlook Express process the encoded script when the email appears in the preview pane (the email does not need to be opened). The script downloads the NetSky worm from known Internet sites and installs the worm on the target host.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>WORM:NIMDA:BIN-255-CMD</td>
<td>This signature detects attempts to infect a Microsoft IIS Web server with the Nimda worm. Nimda may infect other Web servers by obtaining email addresses and sending a copy of itself in infected messages using its own SMTP or POP3 server; adding files to a system configured to allow Windows file shares; or posting an infected HTML email to the Web server where it can be accessed via HTTP.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>WORM:NIMDA:MSADC-ROOT</td>
<td>This signature detects attempts to infect a Microsoft IIS Web server with the Nimda worm. Nimda may infect other Web servers by obtaining email addresses and sending a copy of itself in infected messages using its own SMTP or POP3 server; adding files to a system configured to allow Windows file shares; or posting an infected HTML email to the Web server where it can be accessed via HTTP.</td>
<td>medium</td>
<td>sos5.0.0, sos5.1.0</td>
</tr>
<tr>
<td>WORM:NIMDA:NIMDA-EML</td>
<td>This signature detects attempts to create .EML files on the system, a common sign of the NIMDA worm. The worm browses remote directories and creates .EML files (the worm's multi-part messages containing a MIME-encoded worm) with the same names as existing documents or Web page files.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>WORM:NIMDA:NIMDA-NWS</td>
<td>This signature detects attempts to create a .NWS file on the system, a common sign of the NIMDA worm. The worm browses remote directories and creates .NWS files (the worm's multi-part messages containing a MIME-encoded worm) with the same names as existing documents or Web page files.</td>
<td>medium</td>
<td>sos5.1.0</td>
</tr>
<tr>
<td>WORM:NIMDA:NIMDA-RICHED20</td>
<td>This signature detects attempts to create the file RICHED20.DLL on the system, a common sign of the NIMDA worm. The worm may overwrite the original RICHED20.DLL in the Windows systems folder with a binary copy of itself, and place additional copies in all folders containing .DOC or .EML files.</td>
<td>high</td>
<td>sos5.1.0</td>
</tr>
</tbody>
</table>
### Attack Name | Attack Description | Severity | Versions
--- | --- | --- | ---
**WORM:NIMDA:SCRIPTS-C11C-CMD** | This signature detects attempts to infect a Microsoft IIS Web server with the Nimda worm. Nimda may infect other Web servers by obtaining email addresses and sending a copy of itself in infected messages using its own SMTP or POP3 server; adding files to a system configured to allow Windows file shares; or posting an infected HTML email to the Web server where it can be accessed via HTTP. | medium | sos5.0.0, sos5.1.0

**WORM:NIMDA:SCRIPTS-CMD** | This signature detects attempts to infect a Microsoft IIS Web server with the Nimda worm. Nimda may infect other Web servers by obtaining email addresses and sending a copy of itself in infected messages using its own SMTP or POP3 server; adding files to a system configured to allow Windows file shares; or posting an infected HTML email to the Web server where it can be accessed via HTTP. | medium | sos5.0.0, sos5.1.0

**WORM:NIMDA:SCRIPTS-ROOT** | This signature detects attempts to infect a Microsoft IIS Web server with the Nimda worm. Nimda may infect other Web servers by obtaining email addresses and sending a copy of itself in infected messages using its own SMTP or POP3 server; adding files to a system configured to allow Windows file shares; or posting an infected HTML email to the Web server where it can be accessed via HTTP. | medium | sos5.0.0, sos5.1.0

**WORM:PHPINCLUDE:SEARCH-REQ** | This signature detects the Santy.C worm attempting to find targets by sending a search request to a Google or Yahoo search engine. | medium | sos5.1.0

**WORM:SANTY:GOOGLE-SEARCH** | This signature detects a machine infected with the Santy worm querying Google to locate new targets for infection. The source IP of this log is likely infected with a variant of Santy. | medium | sos5.1.0

**WORM:SANTY:INFECT-ATTEMPT** | This signature detects a machine infected with the Santy worm attempting to infect a new target host. The source IP of this log is likely infected with a variant of Santy. | high | sos5.1.0

**WORM:SMB:DELODER** | This signature detects attempts to upload the deloder worm. This signature also indicates that the worm has already logged into the system; the deloder worm can upload itself to the host only after successful login as Administrator (deloder uses one of 50 default passwords to login). | critical | sos5.1.0

**WORM:SMB:W32-SLACKOR** | This signature detects SMB transmissions of the W32/Slackor worm, which targets file shares. The worm scans the /16 of the infected host for systems listening on TCP/445; if a system is found, the worm uses pre-programmed usernames and passwords to connect to the $IPC share on the system, copies itself to the C:\sp directory, and runs its payload. | high | sos5.1.0

---

**Configuration Log Entries**

The Configuration category contains the following subcategories:
Table 97: Configuration Log Entries

<table>
<thead>
<tr>
<th>Configuration Log Entry Subcategories</th>
<th>ScreenOS Message ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Addresses &gt; Notification &gt; 00001</td>
</tr>
<tr>
<td>Admin</td>
<td>Admin &gt; Notification &gt; 00002</td>
</tr>
<tr>
<td>Auth</td>
<td>Auth &gt; Notification &gt; 00015</td>
</tr>
<tr>
<td>Clock</td>
<td>System &gt; Notification &gt; 00014</td>
</tr>
<tr>
<td>CLS</td>
<td>Notification &gt; 00043</td>
</tr>
<tr>
<td>CMS</td>
<td>Device &gt; Notification &gt; 00022</td>
</tr>
<tr>
<td>Console</td>
<td>Admin &gt; Notification &gt; 00003</td>
</tr>
<tr>
<td>DHCP CLI</td>
<td>DHCP &gt; Notification &gt; 00027</td>
</tr>
<tr>
<td>DHCP IP</td>
<td>DHCP &gt; Notification &gt; 00009</td>
</tr>
<tr>
<td>DHCP Opt</td>
<td>DHCP &gt; Notification &gt; 00024</td>
</tr>
<tr>
<td>DIP</td>
<td>DIP &gt; Notification &gt; 00021</td>
</tr>
<tr>
<td>DNS</td>
<td>DNS &gt; Notification &gt; 00004</td>
</tr>
<tr>
<td>DNS REP</td>
<td>DNS &gt; Notification &gt; 00029</td>
</tr>
<tr>
<td>Erase</td>
<td>System &gt; Notification &gt; 00023</td>
</tr>
<tr>
<td>Hostname</td>
<td>System &gt; Notification &gt; 00006</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface &gt; Notification &gt; 00009</td>
</tr>
<tr>
<td>MIP</td>
<td>MIP &gt; Notification &gt; 00021</td>
</tr>
<tr>
<td>NSRP</td>
<td>High Availability &gt; Notification &gt; 00007</td>
</tr>
<tr>
<td>OSPF</td>
<td>OSPF &gt; Notification &gt; 00038</td>
</tr>
<tr>
<td>PKI</td>
<td>PKI &gt; Notification &gt; 00002</td>
</tr>
<tr>
<td>Policy</td>
<td>Policies &gt; Notification &gt; 00018</td>
</tr>
<tr>
<td>PPP</td>
<td>HDLC &gt; Notification &gt; 00042</td>
</tr>
<tr>
<td>PPPoE</td>
<td>PPPoE &gt; Notification &gt; 00034</td>
</tr>
<tr>
<td>RIP</td>
<td>RIP &gt; Notification &gt; 00045</td>
</tr>
<tr>
<td>Route</td>
<td>Route &gt; Notification &gt; 00011</td>
</tr>
<tr>
<td>Route Map</td>
<td>Route &gt; Notification &gt; 00048</td>
</tr>
<tr>
<td>Schedule</td>
<td>Schedule &gt; Notification &gt; 00020</td>
</tr>
<tr>
<td>Service</td>
<td>Service &gt; Notification &gt; 00012</td>
</tr>
<tr>
<td>Set ARP</td>
<td>ARP &gt; Notification &gt; 00051</td>
</tr>
<tr>
<td>Shaper</td>
<td>Traffic Shaping &gt; Notification &gt; 00002</td>
</tr>
<tr>
<td>SIP ALG</td>
<td>Flow &gt; Notification &gt; 00047</td>
</tr>
<tr>
<td>SME</td>
<td>NSM &gt; Notification &gt; 00033</td>
</tr>
<tr>
<td>SNMP</td>
<td>SNMP &gt; Notification &gt; 00031</td>
</tr>
<tr>
<td>SW Key</td>
<td>Entitlement &gt; Notification &gt; 00036</td>
</tr>
<tr>
<td>SSH</td>
<td>SSHv2 &gt; Notification &gt; 00026</td>
</tr>
<tr>
<td>SSL</td>
<td>SSL &gt; Notification &gt; 00035</td>
</tr>
<tr>
<td>Syslog</td>
<td>Syslog and WebTrends &gt; Notification &gt; 00019</td>
</tr>
<tr>
<td>Track IP</td>
<td>High Availability &gt; Notification &gt; 00050</td>
</tr>
</tbody>
</table>
Information Log Entries

The Information category contains the following subcategories:

Table 98: Information Log Entries

<table>
<thead>
<tr>
<th>Information Log Entry Subcategories</th>
<th>ScreenOS Message ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auth Challenge</td>
<td>Auth &gt; Information &gt; 00546</td>
</tr>
<tr>
<td>Auth Failed</td>
<td>Auth &gt; Warning &gt; 00518</td>
</tr>
<tr>
<td>Auth Status Change</td>
<td>Auth &gt; Information &gt; 00525</td>
</tr>
<tr>
<td>Auth Passed</td>
<td>Auth &gt; Warning &gt; 00519</td>
</tr>
<tr>
<td>Auth Timeout</td>
<td>Auth &gt; Warning &gt; 00520</td>
</tr>
<tr>
<td>Anti Virus</td>
<td>AntiVirus Scanning (External) &gt; Information &gt; 00547</td>
</tr>
<tr>
<td>BGP</td>
<td>BGP &gt; Information &gt; 00542</td>
</tr>
<tr>
<td>Clock</td>
<td>NTP &gt; Notification &gt; 00531</td>
</tr>
<tr>
<td>Configuration Size</td>
<td>System &gt; Notification &gt; 00553</td>
</tr>
<tr>
<td>Device Connect</td>
<td>N/A</td>
</tr>
<tr>
<td>Device Disconnect</td>
<td>N/A</td>
</tr>
<tr>
<td>DHCP CLI</td>
<td>DHCP &gt; Information &gt; 00530</td>
</tr>
<tr>
<td>DHCP DNS</td>
<td>DNS &gt; Information &gt; 00004</td>
</tr>
<tr>
<td>Generic</td>
<td>System &gt; Information &gt; 00767</td>
</tr>
<tr>
<td>VIP Svr Up</td>
<td>VIP &gt; Notification &gt; 00533</td>
</tr>
<tr>
<td>Link Status</td>
<td>Interface &gt; Notification &gt; 00513</td>
</tr>
<tr>
<td>Log Cleared</td>
<td>Logging &gt; Information &gt; 00534</td>
</tr>
<tr>
<td>NSRD</td>
<td>NSRD &gt; Information &gt; 00551</td>
</tr>
<tr>
<td>NTP failure</td>
<td>NTP &gt; Notification &gt; 00531</td>
</tr>
<tr>
<td>NTP timeout</td>
<td>NTP &gt; Notification &gt; 00531</td>
</tr>
<tr>
<td>OSPF</td>
<td>OSPF &gt; Information &gt; 00541</td>
</tr>
<tr>
<td>Password Change</td>
<td>Admin &gt; Information &gt; 00002</td>
</tr>
</tbody>
</table>

The Information category contains the following subcategories:

Table 98: Information Log Entries
<table>
<thead>
<tr>
<th>Subcategories</th>
<th>ScreenOS Message ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>PKI</td>
<td>PKI &gt; Information &gt; 00535</td>
</tr>
<tr>
<td>PPP</td>
<td>PPP &gt; Notification &gt; 00539</td>
</tr>
<tr>
<td>PPPoE</td>
<td>PPPoE &gt; Notification &gt; 00034</td>
</tr>
<tr>
<td>RIP</td>
<td>RIP &gt; Information &gt; 00544</td>
</tr>
<tr>
<td>SME</td>
<td>NSM &gt; Information &gt; 00538</td>
</tr>
<tr>
<td>SNMP</td>
<td>SNMP &gt; Information &gt; 00524</td>
</tr>
<tr>
<td>SSH</td>
<td>SSHv1 &gt; Information &gt; 00528</td>
</tr>
<tr>
<td></td>
<td>SSHv2 &gt; Information &gt; 00026</td>
</tr>
<tr>
<td>SSL</td>
<td>SSL &gt; Information &gt; 00284</td>
</tr>
<tr>
<td>URL Blk</td>
<td>WEB Filtering &gt; Notification &gt; 00523</td>
</tr>
<tr>
<td>Username Change</td>
<td>Admin &gt; Information &gt; 00002</td>
</tr>
<tr>
<td>VPN</td>
<td>VPN &gt; Information &gt; 00536</td>
</tr>
<tr>
<td></td>
<td>L2TP &gt; Information &gt; 00536</td>
</tr>
<tr>
<td></td>
<td>IKE &gt; Information &gt; 00536</td>
</tr>
<tr>
<td>VIP Server Status</td>
<td>VIP &gt; Notification &gt; 00533</td>
</tr>
<tr>
<td>DHCP Server Status</td>
<td>DHCP &gt; Information &gt; 00527</td>
</tr>
</tbody>
</table>

NOTE: For security devices running ScreenOS 5.0.x or higher, NetScreen-Security Manager does not generate information logs for device connect and disconnect events. The Realtime Monitor however, does display the correct up/down status of the device.

Self Log Entries
Self log entries appear in the Log Viewer under the category Self, which contains a single subcategory: Self Log.

Traffic Log Entries
Traffic log entries appear in the Log Viewer under the category Traffic, which contains a single subcategory: Traffic Log.

GTP Log Entries
When you enable logging in a GTP object, you can configure a security device to create log entries with Basic or Extended information. Additionally, when counting is also enabled the GTP object, the device also generates log entries for deleted GTP tunnels.

For log entries generated by GTP objects with Basic logging enabled, you can view the following information:
For log entries generated by GTP objects with Extended logging enabled, you can view the following information:

### Table 99: Basic GTP Log Entry

<table>
<thead>
<tr>
<th>Basic GTP Log Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timestamp</td>
</tr>
<tr>
<td>Source IP address</td>
</tr>
<tr>
<td>Destination IP address</td>
</tr>
<tr>
<td>TID (Tunnel Identifier) or TEID (Tunnel Endpoint Identifier)</td>
</tr>
<tr>
<td>Message type</td>
</tr>
<tr>
<td>Packet status: forwarded, prohibited, state-invalid, rate-limited, or tunnel-limited</td>
</tr>
<tr>
<td>Interface, vsys, or vrouter name (if applicable)</td>
</tr>
<tr>
<td>PLMN or zone name</td>
</tr>
</tbody>
</table>

### Table 100: Extended GTP Log Entry

<table>
<thead>
<tr>
<th>Extended GTP Log Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>IMSI</td>
</tr>
<tr>
<td>MSISDN</td>
</tr>
<tr>
<td>APN</td>
</tr>
<tr>
<td>Selection Mode</td>
</tr>
<tr>
<td>SGSN address for signaling</td>
</tr>
<tr>
<td>SGSN address for user data</td>
</tr>
<tr>
<td>GGSN address for signaling</td>
</tr>
<tr>
<td>GGSN address for user data</td>
</tr>
</tbody>
</table>

### Table 101: Deleted GTP Tunnel Log Entry

<table>
<thead>
<tr>
<th>Deleted GTP Tunnel Log Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timestamp</td>
</tr>
<tr>
<td>Interface name (if applicable)</td>
</tr>
<tr>
<td>SGSN IP address</td>
</tr>
<tr>
<td>GGSN IP address</td>
</tr>
<tr>
<td>TID</td>
</tr>
<tr>
<td>Tunnel duration time in seconds</td>
</tr>
<tr>
<td>Number of messages sent to the SGSN</td>
</tr>
<tr>
<td>Number of messages sent to the GGSN</td>
</tr>
</tbody>
</table>
The Index provides an alphabetical listing of important terms and concepts used in this guide, as well as the page numbers on which those terms and concepts are found.
Index

A
Abstract Data Model .................................................. 215
access lists
defined ................................................................. 675
Access Point Name
See APN
access-challenge, defined........................................... 675
actions, configuring in firewall rules.......................... 334
active sessions
information available............................................ 537–538
session display filter ................................................. 539
session filter.......................................................... 538
viewing................................................................. 537–539
active statistics
about.................................................................... 524
viewing................................................................. 537
active VPN
details, viewing........................................................ 546
information, viewing .............................................. 530
activities
admin roles .......................................................... 66
admins .................................................................... 66
attack update.......................................................... 66
audit logs ............................................................... 66
device certificates................................................... 66
device configuration ................................................ 67
device delta config .................................................. 67
device firmware ....................................................... 67
device log comments ............................................. 67
device log flags ....................................................... 67
device logs............................................................. 67
device passwords ................................................... 67
device reboot .......................................................... 67
device running config ............................................ 67
device software keys .............................................. 67
device status monitor ............................................. 67
device Web categories .......................................... 67
devices, groups, templates ..................................... 67
firewall rulebases .................................................. 67
HA for guiSrvrClusterMgr ..................................... 67
historical reports ..................................................... 67
investigative log reports ........................................ 68
jobs ........................................................................ 68
multicast rulebases ............................................... 68
NSRP Monitor ......................................................... 68
policy lookup table ................................................ 68
rulebases .............................................................. 68
security policies .................................................... 68
servers ................................................................. 68
shared objects and groups ...................................... 68
subdomains and groups ......................................... 69
system Web categories .......................................... 69
VPN Monitor ........................................................ 69
VPNs ..................................................................... 69
Adding the Exempt Rulebase .................................... 364
address objects
about .................................................................. 227
configuring in firewall rules .................................. 331
defined ................................................................. 675
address shifting
defined ................................................................. 675
See NAT-dst, and NAT-src
address spoofing, defined ........................................ 675
adjacencies, defined .............................................. 675
administrative reports .......................................... 652, 655, 656, 667
administrators
creating................................................................. 57
permissions ............................................................ 66
advertisement, defined ........................................... 676
AES
defined ................................................................. 675
aggregate state, defined .......................................... 676
aggregation, defined .............................................. 676
aggregator, defined ................................................ 676
aggressive aging, defined ....................................... 676
alarms, configuring in firewall rules ....................... 339
alerts, configuring in firewall rules ......................... 338
ALG
defined ................................................................. 676
APN filter
about ................................................................... 278
network ID, setting ................................................ 279
selection mode, setting .......................................... 279
APN, defined ........................................................ 676
application relocation, configuring in firewall rules .... 341
area border router, defined .................................... 676
area range, defined ................................................ 676
area, defined ........................................................ 676
AS number, defined .............................................. 676
AS path access list, defined ................................... 676
AS path attribute class, defined ............................. 676
AS path string, defined ......................................... 676
ASN1-DN ............................................................. 445
atomic aggregate, defined ...................................... 677
atomic configuration
about ................................................................... 174
defined ................................................................. 677
atomic updating ..................................................... 174
attack context for custom attack object.................... 250
attack direction for custom attack object ................ 250
attack flow for custom attack object ....................... 250
attack header matches for custom attack object ....... 251
attack name and description for custom attack object 241
attack object
copying predefined ................................................ 241
editing copy of predefined .................................... 241
attack object database
checking version ................................................... 201
managing versions ........................................ 202
permissions.............................................. 66
updating............................................. 198
upating on 4.0.x and 5.0.x devices ............... 200
upating overview .................................... 197
attack object groups ..................................... 259
attack objects
  custom compound ..................................... 244, 255
  custom compound, adding members ............... 257
  custom compound, attack pattern .................. 257
  custom compound, ordered match .................. 257
  custom compound, scope ............................. 256
  custom protocol anomaly ............................ 244, 255
  custom signature ....................................... 244, 245
  custom signature attacks, attack context .......... 250
  custom signature, attack direction ................. 251
  custom signature, attack flow ........................ 251
  custom signature, attack header matches ........... 251
  custom signature, attack pattern .................... 249
  custom signature, attack pattern syntax ............. 249
  custom signature, false positive setting .............. 245
  custom signature, first packet context .............. 250
  custom signature, IP header matches ............... 252
  custom signature, IP protocol and type .............. 246
  custom signature, line context ........................ 251
  custom signature, packet context .................... 250
  custom signature, service binding .................... 245
  custom signature, stream 256 context ............... 251
  custom signature, stream context .................... 250
  custom signature, supported services ............... 247
  custom signature, TCP header matches ............... 253
  custom signature, time binding ....................... 248
  custom signature, UDP header matches ............... 254
  custom, about ........................................... 240
  custom, extended information ....................... 242
  custom, external references ........................ 243
  custom, groups ........................................... 259
  custom, name and description ........................ 241
  custom, target platform ................................ 243
defined .............................................. 677
DI profiles ............................................ 233
local update ........................................... 198
predefined ............................................. 233
updating ............................................... 197
  using proxy .......................................... 200
  updating predefined .................................... 235, 240
  viewing predefined .................................... 234
attack pattern for custom attack object ............. 249
attack pattern syntax ..................................... 249
attack statistics ......................................... 523, 533–536
attack trends, using reports to identify .............. 671
Attacks by Severity (DI) report .......................... 654
Attacks by Severity (Screen) report ..................... 655
Attacks over Time (DI) report .......................... 654
Attacks over Time (Screen) report ..................... 655, 671
Audit Log Viewer
  about .................................................. 23
  before or after updating ................................ 181
  defined .................................................. 677
  introduction ............................................ 172
audit logs, permission to view ........................... 66
authentication
  configuring in firewall rules ........................... 343
  defined .................................................. 677
authentication servers
  backup servers ......................................... 290
  defined .................................................. 677
  objects .................................................. 289
  RADIUS .................................................. 292–296
  RADIUS example ......................................... 294
  RADIUS user support .................................... 293
timeout .................................................. 289
types ....................................................... 291
authentication users
  run-time (external user group) ........................ 300
timeout ................................................... 290
Automatic Device Log Cleanup ............................ 636
autonomic system
  boundary router, defined ............................... 677
  defined .................................................. 677
  path, defined .......................................... 677
AV
  activating subscription on device ...................... 197
  configuring in firewall rules .......................... 344
  profiles .................................................. 265
  scanning, defined ....................................... 676
  update pattern file ..................................... 209
backdoor rulebase
  about .................................................... 367
  adding to Security Policy .............................. 368, 373, 379, 382
backdoor rules
  configuring ............................................. 367–371
  configuring actions ........................................ 370
  configuring Match columns ............................. 368, 373, 379, 383
  configuring notification .................................. 370, 374, 380, 383
  configuring operation ..................................... 369
  configuring services ....................................... 369
  configuring severity ........................................ 371, 376, 381, 384
  configuring source and destination ..................... 369, 373, 379
  configuring zones ......................................... 369
  entering comments ....................................... 371
backup interface, fail over ............................... 212
bastion host, defined .................................... 677
BGP
  defined .................................................. 677
  keepalive, defined ....................................... 683
  neighbor, defined ....................................... 677
  peer connection troubleshooting ......................... 213
  broadcast networks, defined ............................ 678
BugTraq references ........................................ 243
certificate authorities ...................................... 309
changes that affect device connection ................... 148
chart type, configuring ..................................... 664
CIDR, defined ............................................ 678
Classless Inter-Domain Routing, defined ................. 678
classless routing, defined .................................................. 678
CLI commands, displaying .................................................. 214
CLI, defined ................................................................... 678
cluster list for BGP, defined .................................................. 678
command line utilities ......................................................35–??
community for BGP, defined .................................................. 678
compound attack objects
  custom ........................................................................ 255
  custom, adding protocol anomaly ................................. 257
  custom, configuring attack pattern ................................. 257
  custom, configuring ordered match ................................. 257
  custom, configuring scope ............................................ 256
confederation for BGP, defined .................................................. 678
configlet, defined ................................................................ 678
configuration logs report ..................................................654
configuration states .............................................................. 178
configuration summary, running ............................................ 182, 186
configuring
  devices ........................................................................ 143–??
  logging ........................................................................... 587–650
  monitoring ..................................................................... 515–559, 561–??
  objects .......................................................................... 223–318, 503–??
  reporting ......................................................................... 651–672
  role-based administration .............................................. 51–??
  security policies ............................................................ 319–414
  VPNs .............................................................................. 415–502
configuring in rule ............................................................... 346
connection states ................................................................. 178
connections, BGP peer ....................................................... 213
counting, configuring in firewall rules ...................................... 339
CRLs (certificate revocation list) .................................................. 312
customer support ............................................................... xxxvii
CVE references .................................................................. 243
D
dashboard
  about ............................................................................. 562
Data Model
  defined ........................................................................... 215
  importing ........................................................................ 218
  schema .......................................................................... 216
  updating .......................................................................... 216
data model, defined ............................................................. 679
data point count ................................................................. 624, 664
data types ........................................................................... 624
Deep Inspection
  activating subscription on device ....................................... 197
  attack objects, custom .................................................... 240
  checking attack object database ..................................... 201
  local attack object update .............................................. 198
  profiles in firewall rules .................................................. 345
  profiles, about ................................................................ 233
  updating attack object database ....................................... 197
default values in templates .................................................. 151
delta configuration summary .................................................. 182, 186
deny action, configuring in firewall rules ................................. 334
dependant activities ............................................................ 66
DES, defined ...................................................................... 679
DES-CBC, defined .............................................................. 679
destination NAT, configuring in firewall rules ......................... 336
device administrator
  defined ........................................................................... 679
device capabilities
  file ................................................................................. 216
  viewing ........................................................................... 168
device certificates, permissions .............................................. 66
device clock, updating ....................................................... 211
device configuration
  about ............................................................................. 144
  link from Log Viewer ..................................................... 619
  memory optimization ..................................................... 144
  permissions ..................................................................... 67
  unsupported in UI .......................................................... 148
  updating .......................................................................... 185
device connection to Security Manager ...................................... 148
device delta config, permission to view .................................... 67
device firmware
  adjusting version ............................................................ 195
  permission to update ...................................................... 67
device groups
  permissions ...................................................................... 67, 68
  planning for ..................................................................... 45
  using ............................................................................... 165
  device log comments, permission to update ....................... 67
  device log flags, permission to update .............................. 67
  device logs, permissions .................................................. 67
  Device Manager module .................................................. 20, 143
  device monitor, defined .................................................. 679
  device passwords, permission to view ................................ 67
  device policy pointers ..................................................... 396
  device reboot, permission ................................................ 67
  device references, finding ............................................... 214
device running config, permission to view ................................ 67
  Device Server
    about ............................................................................. 14
    defined .......................................................................... 679
    permissions ..................................................................... 68
    processes ......................................................................... 14
    device software keys, permission to install ..................... 67
    device status ................................................................. 178
    device status monitor, permission to view ....................... 67
    device templates ........................................................... 45
    exporting ........................................................................ 164
    importing ......................................................................... 165
  See also templates
  device traffic distribution, viewing ..................................... 524
  device update, errors ..................................................... 191
  devices, configuring in firewall rules .................................... 335
  devices, re-importing ....................................................... 395
  device-specific VPN information, viewing ......................... 546
DHCP
  defined ........................................................................... 679
DI
  See Deep Inspection
DI profiles
  creating ........................................................................... 235
DI reports ...............................................................652, 654
dial backup
  configuring for route-based VPN member ......................... 440
IKE
  defined........................................................... 683
  key management, defined........................................ 684
  proposals........................................................... 316
import rules
  defined........................................................... 682
importing
  device templates................................................ 165
  importing devices............................................... 83
IMSI
  defined........................................................... 682
  prefix filter.................................................... 279
information logs
  report............................................................. 654
inline mode........................................................ 40, 346
inline tap mode.................................................... 40, 346
installing license key on device................................ 196
interface failover
  forcing on device.............................................. 212
interface statistics, viewing.................................... 531
interfaces
  device-specific views, described............................ 523
  statistics.......................................................... 531
  tunnel, defined................................................ 692
intrusion detection and prevention
  See IDP
investigative log reports, permissions........................ 68
IP address, defined............................................... 683
IP gateway, defined.............................................. 688
IP header matches for custom attack object................ 252
IP pools
  configuring.................................................... 303
  defined.......................................................... 683
  using multiple ranges........................................ 303
IP tracking, defined............................................ 683
IP, defined........................................................ 683
IPSec, defined.................................................... 683
ISAKMP, defined.................................................... 683
ISG
  push IDP rulebase only....................................... 391
J
  Job Manager
    about................................................................ 23
    defined.......................................................... 683
  job status logs, permission to purge......................... 68
jobs, permission to view......................................... 68
K
  key list parameters in templates............................ 152
L
  L2TP
    configuring in device-level VPNs............................ 486
    configuring in VPN Manager................................. 437
  lawful interception in GTP object............................ 280
  left axis, Log Investigator................................... 623
  license key
    displaying for device........................................ 196
    installing on device......................................... 196
    obtaining...................................................... 196
  line context for custom attack object....................... 251
  link state advertisement, defined............................ 684
  link state, defined............................................. 684
  linking to a device from Log Viewer......................... 619
  load balancing, defined....................................... 684
  local attack object update.................................... 198
  local preference for BGP, defined............................. 684
  local user groups............................................... 298
  local users...................................................... 429
log actions
  about................................................................ 640
  csv................................................................... 641
  email............................................................... 641
  SNMP.................................................................. 640
  syslog............................................................... 640
  xml................................................................... 641
log categories
  defined............................................................ 684
  filtering in Log Viewer......................................... 612
log criteria............................................................ 641
log destinations
  email server...................................................... 593
  Syslog................................................................ 600
  WebTrends server............................................... 601
log entries
  actions.............................................................. 640
  criteria.............................................................. 640
  enabling in firewall rules..................................... 338
  exporting........................................................... 640
  filtering with ranges........................................... 615
  identifying patterns............................................. 180
  searching by ID.................................................. 612
  severity levels.................................................... 589
  SNMP.................................................................. 599
  using the Find utility.......................................... 611
log ID, defined...................................................... 684
Log Investigator
  about................................................................ 19
  configuring axes............................................... 623
  defined.............................................................. 684
  setting data point count....................................... 624
  setting data types............................................... 624
log severity
  alert.................................................................. 589
critical ................................................................. 589
debugging ............................................................. 591
emergency ............................................................ 589
error ...................................................................... 589
information ........................................................... 590
levels ...................................................................... 589
notification ............................................................ 590
warning .................................................................... 589
log sub-categories .................................................. 591, 603
log types
  config ................................................................. 603
custom ..................................................................... 603
info ......................................................................... 603
screen ...................................................................... 603
self ......................................................................... 603
traffic ...................................................................... 603
Log Viewer
  about ....................................................................... 19
  creating an exempt rule ......................................... 366
  defined ...................................................................... 684
  filtering .................................................................... 612
  find utility .................................................................. 611
  flags ......................................................................... 611
  integration with reports ........................................ 665
  linking to a device .................................................. 619
  log categories ......................................................... 612
  log ID ...................................................................... 612
  log sub-categories .................................................. 612
  saving a view .......................................................... 603
  saving custom views .............................................. 603
  unknown values ..................................................... 606
  using ranges for filtering ....................................... 615
  view ......................................................................... 603
log, defined ............................................................. 684
log2action
  common options .................................................... 643
  exporting to CSV .................................................... 646
  exporting to script .................................................. 649
  exporting to SMTP (email) ...................................... 648
  exporting to SNMP .................................................. 647
  exporting to syslog .................................................. 648
  exporting to XML ..................................................... 645
logging
  configuring in firewall rules .................................... 338
  self log entries ....................................................... 592
Logs by User-set Flag report .................................... 656, 668
loopback interface
  defined ...................................................................... 684

M
main display area .................................................... 18
managed devices ..................................................... 15
manual key ................................................................ 490
MCC, defined ........................................................... 685
MD5, defined ............................................................ 685
Media Gateway Control Protocol, defined ................ 685
member AS, defined .................................................. 685
merging security policies ......................................... 396
meshing, disabling in VPN Manager ......................... 440
metric, defined ........................................................ 685
Microsoft Remote Procedure Call (MS-RPC) .......... 283
MIPs
  defined ...................................................................... 685
  global objects ........................................................ 309
  using in rules ........................................................ 332
MNC, defined ............................................................ 685
Mobile Country Code (MCC) .................................. 279
Mobile Network Code (MNC) .................................. 279
Mobile Subscriber Identification Number (MSIN) .... 279
mode, extended port ............................................... 96, 100
modeling, defined ..................................................... 685
module, defined ........................................................ 685
modules, NetScreen-Security Manager .................... 19
monitoring
  NSRP statistics ....................................................... 547
  VPN Status ............................................................ 545
MS, defined .............................................................. 685
MSIN, defined .......................................................... 685
multicast rulebase
  about ....................................................................... 324
  permissions ............................................................ 68
multicast rules
  configuring ............................................................. 347–349
  deleting .................................................................... 394
  disabling ................................................................... 395
N
NAT objects
  about ....................................................................... 308
  configuring in firewall rules .................................... 336
  DIP, global ............................................................. 308
  in VPNs ................................................................. 429
  MIP, global ............................................................. 309
  VIP, global ............................................................. 309
NAT Traversal ........................................................ 443
navigation tree ........................................................ 18
negating source or destination in firewall rules .......... 332
neighbor for BGP, defined ...................................... 685
NetScreen dictionary file ......................................... 293
NetScreen Redundancy Protocol
  See NSRP
NetScreen-ISG 2000 security system ......................... 144
NetScreen-Security Manager modules ..................... 19
network honeypot rules
  configuring services .............................................. 383
NHTB, configuring in VPN Manager ......................... 439
NSAPI, defined ........................................................ 686
NSGP
  defined ...................................................................... 686
ns-profile ................................................................. 342
NSRP
  defined ...................................................................... 686
  NSRP Monitor ......................................................... 547
  RTOs, defined ........................................................ 689
  statistics monitoring .............................................. 547
NSRP clusters
  creating cluster with existing policy ....................... 128
  monitoring ............................................................. 547
statistics ................................................................. 524
NSRP Monitor, permission to view .......................... 68
NTP
  synchronizing device clock ................................. 211

0
Object Manager
about .................................................................. 21
defined .................................................................. 686

objects
about .................................................................. 225
address .................................................................. 227
attacks, updating predefined ................................. 235, 240
attacks, viewing predefined ................................... 234
authentication servers .......................................... 289
AV profiles .......................................................... 265
certificate authorities ........................................... 309
CRLs .................................................................. 312
custom attack group ............................................. 259
custom attacks ....................................................... 240
custom attacks, compound .................................... 244
custom attacks, extended information ..................... 242
custom attacks, external references ....................... 243
custom attacks, name and description ................... 241
custom attacks, protocol anomaly ......................... 244
custom attacks, signature ...................................... 244
custom attacks, target platform ............................. 243
custom compound attacks ................................... 255
custom compound attacks, adding members .......... 257
custom compound attacks, attack pattern ............. 257
custom compound attacks, ordered match ............. 257
custom compound attacks, scope ......................... 256
custom protocol anomalies .................................. 255
custom signature attack objects, attack context ....... 250
custom signature attacks ....................................... 245
custom signature attacks, attack direction ............. 251
custom signature attacks, attack flow .................... 251
custom signature attacks, attack header matches ...... 251
custom signature attacks, attack pattern ............... 249
custom signature attacks, attack pattern syntax ...... 249
custom signature attacks, false positive setting ...... 245
custom signature attacks, first packet context ......... 250
custom signature attacks, IP header matches .......... 252
custom signature attacks, IP protocol and type .......... 246
custom signature attacks, line context .................. 251
custom signature attacks, packet context ............... 250
custom signature attacks, service binding ............. 245
custom signature attacks, stream 256 context ...... 251
custom signature attacks, stream context ............. 250
custom signature attacks, supported services ......... 247
custom signature attacks, TCP header matches ...... 253
custom signature attacks, time binding ................. 248
custom signature attacks, UDP header matches ...... 254
DI profiles ......................................................... 235
DIP, global .......................................................... 308
group expressions ............................................... 304
group expressions, configuring ............................ 305
GTP ................................................................. 275
IKE proposals ..................................................... 316
imported ............................................................... 226
IP pools .............................................................. 303
MIP, global .......................................................... 309
NAT .................................................................... 308
permissions .......................................................... 68
predefined attacks ................................................ 233
protected resources .............................................. 313
remote settings ..................................................... 307
schedules .............................................................. 232
service groups ...................................................... 284
service objects in firewall rules ............................. 333
services .............................................................. 281
services, adding ..................................................... 283
services, custom .................................................... 283
URL predefined categories .................................. 272
users ................................................................. 298
users, external ....................................................... 299
users, local ........................................................... 298
VIP, global .......................................................... 309
Web custom categories ........................................ 271
one-time-password .............................................. 167
optimizing rulebases using reports ....................... 669
OSPF
  defined .............................................................. 686
  virtual link ......................................................... 693
OTP ................................................................. 167
P
packet context ....................................................... 250
PAT
  See port address translation
  pattern file, updating on device ......................... 208
  peer ................................................................. 686
  perfect forward secrecy ..................................... 317
  permit action, configuring in firewall rules ........... 334
  policies
    See security policies
    policy name, ScreenOS ..................................... 346
    policy validation tool ....................................... 386
  port mapping
    See also NAT-dst
    port mapping, defined .................................... 687
    port modes
      Trust/Untrust/DMZ (Extended) .......................... 89
      port modes, defined ....................................... 687
      port scanning ................................................ 376
PPPoE
  defined .............................................................. 687
  predefined entities in templates ......................... 152
  preference, defined ......................................... 687
  preferred ID, configuring in firewall rules .......... 341
  prefixes, defined ............................................. 687
  prerequisite activities ........................................ 66
  preview tools ..................................................... 181
  primary interface, fail over ............................... 212
  priority levels for traffic shaping ....................... 337
 profiler
  alerts ............................................................... 566
  configuring ....................................................... 564

788
context profiles .......................................................... 565
data viewer .................................................................. 569, 570
MAC view area ............................................................ 574
overview ........................................................................ 562
setting up ........................................................................ 563
starting ........................................................................... 566
time intervals .................................................................. 573
using for keeping networks current .................................. 577
using for network baseline ................................................. 576
using for stopping worms and trojans .............................. 578
protected resources .......................................................... 313, 428
protocol anomaly attack objects, custom ......................... 255
protocol distribution
  device-specific attack objects, custom ......................... 523
  viewing ........................................................................... 527–528

R

RADIUS
  access-challenge, defined ............................................ 675
  authentication server example ......................................... 294
  authentication servers ..................................................... 292–296
  compatibility with RFC 2138 ........................................... 292
  ranges .............................................................................. 615
  Realtime Monitor module .................................................. 22
  rebooting devices ............................................................. 210
  redistribution
    defined ............................................................................ 688
    redistribution list ......................................................... 687
  refreshing DNS entries on devices ................................... 210
  re-importing devices ....................................................... 33, 82, 177, 395
  re-importing policies ....................................................... 395
  reject action
    changed to deny ............................................................ 388
    configuring in firewall rules ............................................. 334
    rekey ........................................................................... 447
    remote authentication dial in user service
      See RADIUS
  report groupings ............................................................. 652
  Report Manager module .................................................. 19
  report time period, configuring ......................................... 664
  reporting options on device
    SNMP .............................................................................. 599
    Weblrends ..................................................................... 601
  reports
    administrative .............................................................. 655
    Attacks by Severity (Di) ................................................... 654
    Attacks by Severity (Screen) .......................................... 655
    Attacks over Time (Di) .................................................... 654
    Attacks over Time (Screen) ............................................. 655
    configuring ................................................................. 663
    Di .................................................................................. 654–655
    FW/VPN ........................................................................ 654
    historical ....................................................................... 672
    Logs by User-set Flag ..................................................... 656
    Screen ............................................................................ 655
    Top Alarms ..................................................................... 654
    Top Attacker (Screen) ..................................................... 655
    Top Attacks (Di) ............................................................. 654
NetScreen-Security Manager 2007.2 Administrator's Guide

about.................................................................322
duplication ......................................................386

S
scan manager, configuring in firewall rules.............345
scans
detecting..........................................................376
other scans ......................................................377
port and network scans...................................376
TCP and UDP scans ........................................377
schedule objects
about............................................................232
configuring in firewall rules.........................340
SCP
defined..........................................................689
Screen reports .................................................652, 655
ScreenOS firmware
adjusting version on device..............................195
upgrading on devices ......................................194
versions supported ...........................................15
ScreenOS policy name .....................................346
SDP, defined ....................................................690
searching for logs by ID ....................................612
searching in UI
about..............................................................25
locating IP addresses .......................................28
locating log entries..........................................608
locating patterns at the beginning of a string ......26
locating patterns within a string .......................26
using regular expressions .............................27
Secure Server Protocol
See SSP
Security Manager
architecture ....................................................11
architecture, Abstract Data Model ....................215
architecture, Data Model .................................215
architecture, device capabilities ........................215
architecture, Device Server.............................14
architecture, distributed data collection .............16
architecture, GUI Server ..................................13
architecture, managed devices .......................15
architecture, management system .................12
architecture, UI ...............................................12
device connection changes .............................148
modules, Audit Log Viewer ...............................23
modules, Device Manager ...............................20
modules, Job Manager .....................................23
modules, Log Investigator ................................19
modules, Log Viewer .......................................19
modules, Object Manager ...............................21
modules, Realtime Monitor ..............................22
modules, Report Manager ...............................19
modules, Security Policies .............................20
modules, Server Manager .............................22
modules, VPN Manager .................................21
SSP ..................................................................17
technical overview ...........................................11
UI, about .......................................................18
UI, main display area ......................................18
UI, navigation tree ..........................................18
UI, status bar ..................................................19
UI, toolbar .......................................................19
security policies
about.............................................................20, 320
assigning to a device .....................................385
changing rule order .......................................394
cut, copy, paste ..............................................394
device policy pointers .................................396
device-specific distribution .........................523
exporting .....................................................399
installing .......................................................350
managing .......................................................391
merging .........................................................46, 396
permissions .....................................................68
re-importing ...............................................395
rule groups ....................................................395
rule shadowing ..............................................387
rulebases ......................................................320
rules ............................................................322
session rematch .............................................390
templates ......................................................328
updating .........................................................390
validating .......................................................386
validation tool ...............................................386
validation, rule duplication .........................386
validation, rule shadowing .........................387
validation, unsupported options .................387
validation, zone mismatch ..........................386
zone exceptions ....................................392
security policy distribution, viewing ..........524–526
self logs ..........................................................591
Server Manager module .................................22
service binding
selecting for custom attack object .................245
supported services ........................................247
service objects
about............................................................281
configuring in firewall rules .......................333
custom ..........................................................283
MS-RPC .........................................................283
Sun-RPC .........................................................283
session display filter
configuring ......................................................539
session filter
active sessions, viewing .................................538
session limiting .............................................378
session rematch ............................................390
session timeout, idle timeout .......................290
SHA-1, defined .............................................690
signature attack objects
BugTraq references .......................................243
creating ICMP header properties ...................254
custom ..........................................................245
CVE references ..............................................243
packet context ..............................................250
viewing flow properties ................................251
viewing service binding ..............................246
SIP
defined ..........................................................690
using external user groups in VPNs ...................................... 299
using MIPs as source or destination in firewall rules ........... 332

V
vendor-specific attributes
See VSAs

version of attack object database .................................... 201

VIPs
global objects .................................................................. 309
virtual link, defined ....................................................... 693
virtual security devices
See VSD

virus pattern file, updating on device ................................. 208

VPN links, in firewall rules .............................................. 324

VPN Manager
about ........................................................................... 21, 416
adding policy-based members .......................................... 436
adding RAS users .......................................................... 438
adding routing-based members ....................................... 439
adding the VPN ............................................................ 435
adding the VPN link ....................................................... 450
autogenerating VPN rules ................................................ 448
configuring ASN1-DN ..................................................... 445
configuring FQDN .......................................................... 446
configuring gateway ........................................................ 442
configuring gateway security .......................................... 444
configuring gateway, heartbeats .................................... 442
configuring gateway, mode ............................................ 442
configuring gateway, NAT Traversal ............................... 443
configuring IKE IDs ......................................................... 445
configuring IKE properties ............................................... 446
configuring L2TP ............................................................ 437
configuring NAT ............................................................. 436
configuring NAT with incoming DIP ............................... 436
configuring NAT with MIP, VIP, and Outgoing DIP ....... 437
configuring NAT with tunnel interface and zone .......... 437
configuring overrides ..................................................... 448
configuring overrides, device configuration .................... 449
configuring overrides, policy rules .................................. 448
configuring Phase 1 proposals ........................................ 444
configuring Phase 2 proposals ........................................ 447
configuring PKI .............................................................. 444
configuring preshared key ............................................. 444
configuring preshared secrets ......................................... 445
configuring termination points ....................................... 442
configuring topology ......................................................... 440
configuring topology, full mesh ....................................... 440
configuring topology, hub and spoke ............................. 441
configuring topology, main and branch .......................... 441
configuring topology, site-to-site ................................... 441
configuring XAuth .......................................................... 443
creating VPNs ............................................................... 434
default termination point ................................................ 435
device tunnel summary .................................................... 450
editing VPNs ................................................................. 451
enable dial backup ......................................................... 435
enabling a VPN ............................................................. 435
enabling VPN Monitor ................................................... 447
enabling VPN Monitor, rekey .......................................... 447

examples ..................................................................... 452–474
expanded view .............................................................. 416, 451
view properties ............................................................. 435

VPN Monitor
about ............................................................................. 545
enabling ................................................................. 447
permission to view ......................................................... 69

VPN rules in firewall rulebase ........................................... 324

VPN status summary, viewing ........................................ 545

VPNs
creating with VPN Manager ........................................... 434
device-level, about ....................................................... 417
device-level, adding VPN rules ...................................... 488
device-level, AutoKey IKE VPNs .................................... 475
device-level, L2TP VPNs ............................................... 486
device-level, L2TP-over-AutoKey IKE VPNs.................. 487
device-level, manual key VPNs ..................................... 482
device-level, supported configurations .......................... 474
display filter ................................................................. 546
distribution device-specific view .................................... 523
monitoring status .......................................................... 545
permissions ................................................................. 69
planning for ............................................................... 417
planning for, full mesh .................................................. 420
planning for, hub and spoke ......................................... 419
planning for, IPsec ......................................................... 421
planning for, L2TP ......................................................... 423
planning for, policy-based ........................................... 424
planning for, route-based .............................................. 424
planning for, site-to-site ............................................... 418
preparing certificates ...................................................... 433
preparing group IKE IDs ............................................... 431
preparing NAT objects .................................................... 429
preparing protected resources ........................................ 428
preparing RAS users ..................................................... 429
preparing VPN Components .......................................... 427
supported configurations .............................................. 417
tunneling, defined ........................................................ 692

VSAs
attribute name ............................................................ 294
attribute number .......................................................... 294
attribute type ............................................................. 294
NetScreen dictionary file ............................................... 293
vendor ID ................................................................. 294

W
Web Categories ............................................................ 271
Web categories
permission to update on device ....................................... 67
permission to update on system ..................................... 69
updating on device ....................................................... 209
updating on system ...................................................... 209

Web filtering
black list ..................................................................... 273, 342
block action ................................................................. 273
configuring in firewall rules .......................................... 341
create custom category ................................................ 271
create custom profile .................................................... 273
custom profiles ............................................................ 273
custom Web categories ...........................................342
ns-profile .............................................................274
permissions to update Web categories .................67
permit action ...........................................................273
predefined profiles .............................................273
predefined Web categories .................................272, 342
SurfControl CPA (Integrated) in rules ....................341
SurfControl SCFP/WebSense (Redirect) in rules ......341
white list ..........................................................273, 342
Web Profiles .....................................................273
WebAuth
  configuring in firewall rules ...............................343
WebTrends
  configuring on device ......................................601
defined ....................................................................693
WINS, defined .......................................................693
X
XAuth, defined .....................................................694
Z
zone
  device-specific views .......................................524
exceptions in firewall rules ...............................392
mismatch ............................................................386
statistics .............................................................536
tunnel .....................................................................692