



---

# Network and Security Manager

## Configuring ScreenOS Devices Guide

Release  
2012.2



Modified: 2015-08-04  
Revision 02

Juniper Networks, Inc.  
1133 Innovation Way  
Sunnyvale, California 94089  
USA  
408-745-2000  
[www.juniper.net](http://www.juniper.net)

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

*Network and Security Manager Configuring ScreenOS Devices Guide*  
Release 2012.2  
Copyright © 2015, Juniper Networks, Inc.  
All rights reserved.

Revision History  
January 2013 —01  
August 2015 —02

The information in this document is current as of the date on the title page.

#### YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

#### END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <http://www.juniper.net/support/eula.html>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

# Table of Contents

	<b>About This Guide</b> .....	<b>xv</b>
	Objectives .....	xv
	Audience .....	xv
	Conventions .....	xv
	Documentation .....	xvii
	Requesting Technical Support .....	xviii
<b>Part 1</b>	<b>Configuring</b>	
<b>Chapter 1</b>	<b>NSM User Interface and NSM Key Management Features</b> .....	<b>3</b>
	NSM Overview .....	4
	Security Integration Management Using NSM Overview .....	4
	Complete Support .....	4
	Network Organization .....	5
	Role-Based Administration .....	5
	Centralized Device Configuration .....	5
	Migration Tools .....	6
	Managing Devices in a Virtual Environment Using NSM .....	6
	Device Modeling .....	7
	Rapid Deployment (RD) .....	7
	Policy-Based Management .....	7
	Error Prevention, Recovery, and Audit Management Using NSM .....	8
	Device Configuration Validation .....	9
	Policy Validation .....	9
	Atomic Configuration and Updating .....	9
	Device Image Updates .....	9
	Auditing .....	9
	Administering ScreenOS Devices Using NSM Complete System	
	Management .....	10
	VPN Abstraction .....	10
	Integrated Logging and Reporting .....	11
	Monitoring Status .....	11
	Job Management .....	11
	NSM User Interface Overview .....	12
	Configuring UI Preferences .....	12
	Understanding NSM User Interface Menus and Toolbars .....	12
	Working with Multiple NSM Administrators Overview .....	13
	NSM Modules Overview .....	13
	Navigation Tree .....	14
	Main Display Area .....	14

	Investigate Task Modules in the NSM User Interface Overview . . . . .	14
	Log Viewer . . . . .	14
	Report Manager . . . . .	15
	Log Investigator . . . . .	15
	Realtime Monitor . . . . .	15
	Security Monitor . . . . .	16
	Audit Log Viewer . . . . .	16
	Configure Task Modules in the NSM User Interface Overview . . . . .	16
	Device Manager . . . . .	16
	Security Policies . . . . .	17
	VPN Manager . . . . .	17
	Object Manager . . . . .	18
	Administer Task Modules in the NSM User Interface Overview . . . . .	20
	Server Manager . . . . .	20
	Job Manager . . . . .	20
	Action Manager . . . . .	20
	Understanding Validation Icons and Validation Data in the NSM User Interface . . . . .	21
	Understanding the Search Function in the NSM User Interface . . . . .	22
<b>Chapter 2</b>	<b>Device Configuration . . . . .</b>	<b>25</b>
	Device Configuration Settings Overview . . . . .	25
	About Configuring Security Devices . . . . .	26
	About Configuring Extranet Devices . . . . .	26
	Configuring Advanced Properties for ScreenOS Device Details . . . . .	26
	Configuring a Blacklisted Entry (NSM Procedure) . . . . .	27
	Enabling ALGs (NSM Procedure) . . . . .	28
	Understanding Device Configurations Running ScreenOS 5.4 FIPS and Later Overview . . . . .	29
	About Configuring Devices Running Future Releases of ScreenOS . . . . .	29
	Configuring Extranet Devices Overview . . . . .	30
	Configuring Extranet Devices Details (NSM Procedure) . . . . .	30
	Understanding Templates and Groups . . . . .	32
	Using Global Device Templates . . . . .	33
	Using Device Groups . . . . .	33
	Configuring Network Settings Options and Descriptions . . . . .	34
<b>Chapter 3</b>	<b>Network Settings . . . . .</b>	<b>37</b>
	Configuring Zones and Zone Properties in ScreenOS Devices Overview . . . . .	39
	Predefined Screen Options Overview . . . . .	40
	Configuring Flood Defense Settings for Preventing Attacks . . . . .	41
	Configuring ICMP Flooding Protection . . . . .	41
	Configuring SYN Flooding Protection . . . . .	41
	Configuring UDP Flooding Protection . . . . .	42
	Example: Configuring UDP Flooding Protection (NSM Procedure) . . . . .	43
	HTTP Components and MS-Windows Defense Method . . . . .	43
	Protection Against Scans, Spoofs, and Sweeps . . . . .	44
	IP and TCP/IP Anomaly Detection . . . . .	45
	Prevention of Security Zones Using Denial of Service Attacks . . . . .	47

Malicious URL Protection .....	49
Example: Enabling the Malicious URL Blocking Option (NSM Procedure) .....	50
Interface Types in ScreenOS Devices Overview .....	50
Configuring Physical and Function Zone Interfaces in ScreenOS Devices	
Overview .....	52
Setting Interface Properties Using the General Properties Screen .....	53
Setting WAN Properties Using the WAN Properties Screen .....	54
Setting Port Properties Using the Port Properties Screen .....	54
Using MLFR and MLPPP Options .....	55
Setting Physical Link Attributes for Interfaces .....	55
Enabling Management Service Options for Interfaces .....	56
Setting DHCPv6 Overview .....	57
Example: Assigning TCP/IP Settings for Hosts Using DHCP (NSM Procedure) ..	58
Configuring Custom DHCP Options (NSM Procedure) .....	59
Using Interface Protocol .....	61
Using Interface Secondary IP .....	61
Enabling ScreenOS Devices for Interface Monitoring .....	61
Supporting Generic Routing Encapsulation Using Tunnel Interfaces .....	62
Interface Network Address Translation Methods .....	62
Interface Network Address Translation Using MIPs .....	62
Example: Configuring MIPs (NSM Procedure) .....	63
Interface Network Address Translation Using VIPs .....	65
Mapping Predefined and Custom Services in a VIP .....	65
Example: Configuring VIPs (NSM Procedure) .....	66
Interface Network Address Translation Using DIPs .....	67
Example: Enabling Multiple Hosts Using Port Address Translation (NSM	
Procedure) .....	68
Example: Translating Source IP Addresses into a Different Subnet (NSM	
Procedure) .....	69
Enabling Managed Devices Using Incoming DIP .....	73
Example: Configuring Interface-Based DIP (NSM Procedure) .....	74
Example: Configuring DIP Pools on the Untrust Interface (NSM Procedure) . . .	75
Example: Configuring an Aggregate Interface (NSM Procedure) .....	77
Example: Configuring a Multilink Interface (NSM Procedure) .....	78
Example: Configuring a Loopback Interface (NSM Procedure) .....	79
Configuring Virtual Security Interfaces .....	80
Example: Configuring a Redundant Interface (NSM Procedure) .....	80
Example: Configuring a Subinterface (NSM Procedure) .....	84
Example: Configuring a WAN Interface (NSM Procedure) .....	86
Configuring a Tunnel Interface .....	87
Using Numbered Tunnel Interfaces .....	87
Using Unnumbered Tunnel Interfaces .....	87
Configuring Maximum Transmission Unit Size .....	88
ADSL Interface in ScreenOS Devices .....	88
ADSL, ADSL Interface, and ADSL Settings in ScreenOS Devices .....	89
About ADSL .....	89
About the ADSL Interface .....	89
ADSL Settings from the Service Provider .....	89

	Determining Physical Ports and Logical Interfaces and Zones Using ScreenOS Devices Port Mode . . . . .	91
	Backup Connection Using the Untrusted Ethernet Port in ScreenOS Devices . . .	92
	Example: Configuring NetScreen5GT Devices to Permit Internal Hosts (NSM Procedure) . . . . .	93
	Example: Configuring NetScreen5GT Devices to Connect to the Web Using the PPPoA and ADSL Interfaces (NSM Procedure) . . . . .	94
	Example: Configuring NetScreen5GT Devices as a Firewall Using the PPPoE and ADSL Interfaces (NSM Procedure) . . . . .	96
	Wireless Interface on ScreenOS Devices Overview . . . . .	99
	Configuring DSCP Options Overview . . . . .	99
	Example: Configuring DIP Groups (NSM Procedure) . . . . .	100
	DNS Server Configuration Using DNS Settings . . . . .	103
	Configuring DNS Settings . . . . .	103
	Configuring DNS Proxy . . . . .	104
	Example: Configuring DNS Proxy Entries (NSM Procedure) . . . . .	105
	Example: Configuring DDNS Settings (NSM Procedure) . . . . .	106
	Advanced Network Settings Overview . . . . .	108
	Configuring ARP Cache Entries . . . . .	108
	Configuring VIP Options . . . . .	108
	Configuring DIP Options . . . . .	109
<b>Chapter 4</b>	<b>Advanced Network Settings . . . . .</b>	<b>111</b>
	Configuring Advanced Device Settings Overview . . . . .	112
	Example: Defining Forced Timeout (NSM Procedure) . . . . .	112
	Identifying Reasons for Session Close in NSM . . . . .	113
	Configuring Policy Schedules (NSM Procedure) . . . . .	114
	Configuring Timeouts for Predefined Services (NSM Procedure) . . . . .	115
	Configuring Session Cache for Predefined Services (NSM Procedure) . . . . .	115
	Configuring SIP Settings . . . . .	116
	Configuring MGCP Settings . . . . .	118
	Configuring H.323 Settings . . . . .	119
	Allocating Network Bandwidth Using Traffic Shaping Options . . . . .	119
	Enabling/Disabling Application Layer Gateway Protocols Overview . . . . .	121
	Using Packet Flow Options . . . . .	122
	ICMP Path MTU Discovery . . . . .	123
	Allow DNS Reply Without Matched Request . . . . .	123
	Allow MAC Cache for Management Traffic . . . . .	124
	Allow Unknown MAC Flooding . . . . .	124
	Skip TCP Sequence Number Check . . . . .	124
	TCP RST Invalid Session . . . . .	124
	Check TCP SYN Bit Before Create Session . . . . .	125
	Check TCP SYN Bit Before Create Session for Tunneled Packets . . . . .	125
	Use SYN-Cookie for SYN Flood Protection . . . . .	125
	Enforce TCP Sequence Number Check on TCP RST Packet . . . . .	126
	Use Hub-and-Spoke Policies for Untrust MIP Traffic . . . . .	126
	Max Fragmented Packet Size . . . . .	127
	Flow Initial Session Timeout (Seconds) . . . . .	127
	Multicast Flow Configuration . . . . .	127

TCP MSS . . . . .	127
All TCP MSS . . . . .	127
GRE In TCP MSS . . . . .	128
GRE Out TCP MSS . . . . .	128
Aging . . . . .	128
Early Ageout Time Before the Session's Normal Ageout . . . . .	129
Percentage of Used Sessions Before Early Aging Begins . . . . .	129
Percentage of Used Sessions Before Early Aging Stops . . . . .	129
Configuring Features Unsupported in NSM Using Supplemental CLI Options	
Overview . . . . .	129
Configuring ScreenOS with TFTP or FTP Servers Enabled Using TFTP/FTP	
Options . . . . .	130
Configuring Hostnames and Domain Names Overview . . . . .	130
Configuring NSGP Overview . . . . .	131
NSGP Modules Overview . . . . .	131
Example: Configuring NSGP on GTP and Gi Firewalls (NSM Procedure) . . . . .	132
Using the PPP Option to Configure Point-To-Point Protocol Connections . . . . .	134
About Configuring PPPoE . . . . .	135
Example: Updating DNS Servers (NSM Procedure) . . . . .	136
Example: Configuring Multiple PPPoE Sessions on a Single Interface (NSM	
Procedure) . . . . .	138
Configuring a PPPoA Client Instance . . . . .	141
Configuring a NetScreen Address Change Notification . . . . .	141
Interface Failover in ScreenOS Devices . . . . .	141
Example: Configuring Modem Connections (NSM Procedure) . . . . .	142
Example: Creating Modem Settings (NSM Procedure) . . . . .	143
Example: Creating ISP Connection Settings (NSM Procedure) . . . . .	143
Setting ISP Priority for Failover . . . . .	144
<b>Chapter 5 Administration . . . . .</b>	<b>145</b>
Device Administration Options for ScreenOS Devices Overview . . . . .	146
Importing Device Administrators from a Physical Device Overview . . . . .	146
Device Administrator Authentication Overview . . . . .	147
Device Administrator Account Configuration Overview . . . . .	148
Configuring Privilege Level . . . . .	148
Configuring Authentication . . . . .	149
Admin Access Lock Setting . . . . .	150
Roles for Device Administrator Accounts . . . . .	151
Supporting Admin Accounts for Dialup Connections . . . . .	151
Restricting Management Connections Using Permitted IPs . . . . .	152
Local Access Configuration Using CLI Management Overview . . . . .	153
File Formatting in NSM Overview . . . . .	153
Port Numbers for SSH and Telnet Connections in NSM Overview . . . . .	154
Limiting Login Attempts, Setting Dial-In Authentication, and Restricting Password	
Length in NSM Overview . . . . .	154
Asset Recovery and Reset Hardware in NSM Overview . . . . .	155
Console-Only Connections in NSM Overview . . . . .	156

	Secure Shell Server in NSM Overview . . . . .	156
	Using SSH Version 1 (SSHv1) . . . . .	157
	Using SSH Version 2 (SSHv2) . . . . .	157
	Configuring CLI Banners in NSM Overview . . . . .	158
	Configuring Remote Access Using Web Management Overview . . . . .	159
	Configuring HTTP Administrative Connections in ScreenOS Devices Using NSM Overview . . . . .	159
	Configuring Secure Connections in ScreenOS Devices Using NSM Overview . . .	160
	Configuring Network Time Protocol and NTP Backup Server in NSM Overview . . . . .	161
	Configuring Network Time Protocol . . . . .	162
	Configuring an NTP Backup Server . . . . .	162
	Setting ScreenOS Authentication Options Using General Auth Settings . . . . .	163
	Clearing RADIUS Sessions . . . . .	163
	Assigning an Authentication Request Interface . . . . .	163
	Setting ScreenOS Authentication Options Using Banners Overview . . . . .	164
	Setting ScreenOS Authentication Options Using Default Servers Overview . . .	165
	Setting ScreenOS Authentication Options Using Infranet Settings Overview . . .	165
	General Report Settings for ScreenOS Devices Overview . . . . .	166
	Configuring Syslog Host Using NSM (NSM Procedure) . . . . .	167
	Configuring SNMPv3 in ScreenOS Devices (NSM Procedure) . . . . .	168
<b>Chapter 6</b>	<b>Security . . . . .</b>	<b>173</b>
	Classification of Security Options Overview . . . . .	174
	Classification of Antivirus Scanning Overview . . . . .	174
	External Antivirus Scanner Settings Overview . . . . .	175
	Internal Antivirus Scan Manager Settings Overview . . . . .	176
	Internal Antivirus HTTP Webmail Settings Overview . . . . .	179
	Antivirus Scanner Settings Overview . . . . .	179
	Classification of Deep Inspection Methods . . . . .	181
	Attack Object Database Overview . . . . .	182
	Using Attack Objects Overview . . . . .	183
	Antispam Settings in ScreenOS Overview . . . . .	184
	Configuring Antispam Settings in ScreenOS (NSM Procedure) . . . . .	185
	Configuring IDP Security Module Settings in ScreenOS Overview . . . . .	187
	Load-Time Parameters . . . . .	187
	Run-Time Parameters . . . . .	187
	Protocol Thresholds and Configuration . . . . .	187
	Configuring Integrated Web Filtering in ScreenOS (NSM Procedure) . . . . .	188
	Example: Configuring Integrated Web Filtering (NSM Procedure) . . . . .	188
	Redirect Web Filtering in ScreenOS Using NSM Overview . . . . .	190
	Example: Configuring Redirect Web Filtering in ScreenOS (NSM Procedure) . . .	191
	Adding Proxy Addresses Overview . . . . .	192
<b>Chapter 7</b>	<b>Planning and Preparing VPNs . . . . .</b>	<b>193</b>
	System-Level and Device-Level VPN Using NSM Overview . . . . .	194
	System-Level VPN with VPN Manager Overview . . . . .	194
	Device-Level VPN in Device Manager Overview . . . . .	195
	VPN Configuration Supported Overview . . . . .	196
	Planning Your VPN Using NSM Overview . . . . .	196



Defining VPN Members and Topology Using NSM . . . . .	198
Traffic Protection Using Tunneling Protocol in NSM Overview . . . . .	200
Traffic Protection Using IPsec Tunneling Protocol Overview . . . . .	201
Using Authentication . . . . .	201
Using Encapsulating Security Payload (ESP) . . . . .	201
Traffic Protection Using L2TP Tunneling Protocol Overview . . . . .	203
VPN Tunnel Types Overview . . . . .	203
About Policy-Based VPNs . . . . .	204
About Route-Based VPNs . . . . .	204
Defining VPN Checklist Overview . . . . .	205
Defining Members and Topology in NSM . . . . .	205
Defining Traffic Types for Data Protection in NSM . . . . .	205
Defining VPN Traffic Using Security Protocols in NSM . . . . .	206
Defining Tunnel Creation Methods in NSM . . . . .	206
Using VPN Manager . . . . .	206
Creating Device-Level VPNs . . . . .	207
Preparing Basic VPN Components . . . . .	208
Preparing Required Policy-Based VPN Components Overview . . . . .	209
Policy-Based VPN Creation Using Address Objects and Protected Resources	
Overview . . . . .	209
Configuring Address Objects . . . . .	209
Configuring Protected Resources . . . . .	209
Policy-Based VPN Creation Using Shared NAT Objects Overview . . . . .	210
Policy-Based VPN Creation Using Remote Access Server Users Overview . . . . .	211
Authenticating RAS Users . . . . .	211
Configuring Group IKE IDS . . . . .	212
Configuring Required Routing-Based VPN Components Overview . . . . .	213
Routing-Based VPN Support Using Tunnel Interfaces and Tunnel Zones	
Overview . . . . .	213
Routing-Based VPN Support Using Static and Dynamic Routes Overview . . . . .	214
Preparing Optional VPN Components Overview . . . . .	214
Optional VPN Support Using Authentication Servers Overview . . . . .	215
Optional VPN Support Using Certificate Objects Overview . . . . .	215
Configuring Local Certificates . . . . .	215
Configuring CA Objects . . . . .	216
Configuring CRL Objects . . . . .	216
<b>Chapter 8 Configuring VPNs . . . . .</b>	<b>217</b>
Device Level VPN Types and Supported Configurations Overview . . . . .	219
Device Level AutoKey IKE VPN: Using Gateway Configuration Overview . . . . .	219
ScreenOS Devices Gateway Properties . . . . .	220
ScreenOS Devices IKE IDs or XAuth Identification Number . . . . .	222
Security Methods for ScreenOS Devices . . . . .	224
Device Level AutoKey IKE VPN: Using Routes Configuration Overview . . . . .	225
Device-Level AutoKey IKE VPN: Using VPN Configuration Overview . . . . .	225
Device-Level AutoKey IKE VPN Properties . . . . .	226
ScreenOS Security Measures Using VPN Configuration . . . . .	226
Binding/ProxyID . . . . .	227
Monitor Management on ScreenOS Devices Using AutoKey IKE VPN . . . . .	228

Device-Level AutoKey IKE VPN: Using VPN Rule Configuration Overview . . . . .	228
Device-Level Manual Key VPN: Using XAuth Users Overview . . . . .	229
Device-Level Manual Key VPN: Using Routing-Based VPN Overview . . . . .	229
Device-Level Manual Key VPN: Using VPN Configuration Overview . . . . .	230
Device-Level Manual Key VPN Properties . . . . .	230
Binding . . . . .	231
Monitor Management on ScreenOS Devices Using Manual Key VPN . . . . .	231
Device Level Manual Key VPN: Using VPN Rule Configuration Overview . . . . .	232
Device Level L2TP VPN: Using L2TP Users Configuration Overview . . . . .	233
Device Level L2TP VPN: Using L2TP Configuration Overview . . . . .	233
Device Level L2TP VPN: Using VPN Rule Configuration Overview . . . . .	234
Creating Device Level L2TP-over-Autokey IKE VPNs Overview . . . . .	235
Adding VPN Rules to a Security Policy Overview . . . . .	235
Configuring the VPN . . . . .	235
Configuring the Security Policy . . . . .	236
Assigning and Installing the Security Policy . . . . .	236
Example: Creating Device Level VPN Type 1 (NSM Procedure) . . . . .	236
Example: Creating Device Level VPN Type 2 (NSM Procedure) . . . . .	241
Example: Creating Device Level VPN Type 3 (NSM Procedure) . . . . .	242
L2TP and Xauth Local Users Configuration Overview . . . . .	244
Configuring L2TP Local Users (NSM Procedure) . . . . .	245
XAuth Users Authentication Overview . . . . .	247
Vsys Configurations in NSM Overview . . . . .	248
Virtual Router Configurations for Root and Vsys Overview . . . . .	248
Zone Configurations for Root and Vsys Overview . . . . .	249
Interface Configurations for Root and Vsys Overview . . . . .	251
Viewing Root and Vsys Configurations . . . . .	252
Managing Inter-Vsys Traffic with Shared DMZ Zones . . . . .	252
Example: Routing Traffic to Vsys Using VLAN IDs (NSM Procedure) . . . . .	252
Example: Routing Traffic to Vsys Using IP Classification (NSM Procedure) . . . . .	255
Layer 2 Vsys Configuration Overview . . . . .	257
Assigning L2V VLAN IDs (NSM Procedure) . . . . .	258
L2V VLAN Groups in NSM Overview . . . . .	258
Predefined L2V Zones in NSM Overview . . . . .	259
L2V Interface Management in NSM Overview . . . . .	260
Configuring L2V VLAN Management Interfaces . . . . .	260
Configuring L2V Aggregate Interfaces . . . . .	260
Converting L2V to VLAN Trunking (NSM Procedure) . . . . .	261
Configuring Crypto-Policy Overview . . . . .	264
Certificate Authentication Support in NSM Overview . . . . .	265
Self-Signed Certificates in NSM Overview . . . . .	266
Local Certificate Validation of ScreenOS Devices Overview . . . . .	266
Generating Certificate Requests to ScreenOS Devices (NSM Procedure) . . . . .	267
Loading Local Certificate into NSM Management System . . . . .	269
Installing Local Certificates Using SCEP in NSM . . . . .	270
Manual Installation of Local Certificates in NSM . . . . .	270
Certificate Authority Configuration in NSM Overview . . . . .	271
Installing CA Certificates Using SCEP in NSM . . . . .	271
Manual Installation of CA Certificates in NSM . . . . .	272

	Configuring Certificate Revocation Lists (NSM Procedure) . . . . .	273
	Imported Certificates in NSM Overview . . . . .	273
	PKI Default Settings Configuration in NSM Overview . . . . .	274
	Configuring X509 Certificates . . . . .	274
	Configuring Revocation . . . . .	274
	Configuring Simple Certificate Enrollment Protocol . . . . .	275
<b>Chapter 9</b>	<b>Voice Over Internet Protocol . . . . .</b>	<b>277</b>
	SCCP Support in ScreenOS Devices Overview . . . . .	277
	Configuring SCCP ALG in ScreenOS Devices (NSM Procedure) . . . . .	278
	SIP ALG Overview . . . . .	279
	SIP Request Methods Supported in ScreenOS Devices . . . . .	280
	Types of SIP Response Classes Supported in ScreenOS Devices . . . . .	282
	ALG Overview . . . . .	284
	Configuring SIP ALG in ScreenOS Devices (NSM Procedure) . . . . .	285
	SDP Session Description Overview . . . . .	286
	Pinhole Creation in ScreenOS Devices Overview . . . . .	287
	Session Inactivity Timeout in ScreenOS Devices Overview . . . . .	288
<b>Chapter 10</b>	<b>Routing . . . . .</b>	<b>291</b>
	Configuring Virtual Routers . . . . .	292
	Route Types Overview . . . . .	293
	Virtual Routers Overview . . . . .	294
	Configuring Virtual Routers (NSM Procedure) . . . . .	294
	Virtual Router General Properties Overview . . . . .	295
	Access List Overview . . . . .	296
	Example: Configuring Access Lists (NSM Procedure) . . . . .	297
	Route Map Overview . . . . .	298
	Export and Import Rules in a Virtual Router Overview . . . . .	300
	Example: Configuring Export Rules in a Virtual Router (NSM Procedure) . . . . .	301
	Routing Table Entries Overview . . . . .	303
	Destination-Based Routes Overview . . . . .	305
	Source-Based Routes Overview . . . . .	306
	Example: Configuring Source-Based Routes (NSM Procedure) . . . . .	306
	Source Interface-Based Routes Overview . . . . .	307
	Example: Source-Interface-Based Routing (NSM Procedure) . . . . .	308
	Configuring Route Preferences . . . . .	310
	Dynamic Routing Configuration Overview . . . . .	311
	OSPF Protocol Configuration Overview . . . . .	311
	Enabling OSPF (NSM Procedure) . . . . .	312
	Global OSPF Settings Overview . . . . .	313
	Configuring OSPF Parameters . . . . .	313
	Configuring OSPF Areas . . . . .	314
	Configuring OSPF Summary Import . . . . .	314
	Configuring OSPF Redistribution Rules . . . . .	314
	Configuring OSPF Virtual Links . . . . .	315
	Configuring OSPF Interface Parameters Overview . . . . .	315
	Configuring OSPF Neighbors . . . . .	317
	Configuring OSPF Authentication . . . . .	317
	Configuring OSPF (NSM Procedure) . . . . .	318

RIP Overview . . . . .	319
Configuring RIP (NSM Procedure) . . . . .	320
Global RIP Settings Overview . . . . .	321
Configuring RIP Parameters . . . . .	321
Configuring RIP Redistribution Rules . . . . .	323
Configuring RIP Summary Import (ScreenOS 5.1 and later only) . . . . .	323
RIP Interface Parameters Overview . . . . .	323
Configuring RIP Authentication . . . . .	324
BGP Overview . . . . .	325
Route-Refresh Capabilities Overview . . . . .	326
Configuring BGP Networks . . . . .	327
Configuring Aggregate Addresses . . . . .	327
Configuring Neighbors and Peer Groups Overview . . . . .	328
Configuring a BGP Routing Instance (NSM Procedure) . . . . .	329
Configuring NHRP Overview . . . . .	330
Configuring OSPFv3 Overview . . . . .	331
OSPFv3 Support in Virtual Routers . . . . .	331
OSPFv3 Support in Interfaces . . . . .	332
OSPFv3 Area Parameters . . . . .	332
Redistribution Rules . . . . .	332
OSPFv3 Interface Parameters . . . . .	332
OSPFv3 Route Preference . . . . .	333
Configuring RIPng Overview . . . . .	334
RIPng Parameters . . . . .	334
Redistribution Rules . . . . .	335
Multicast Route Overview . . . . .	335
Configuring IGMP (NSM Procedure) . . . . .	336
Configuring IGMP Proxy (NSM Procedure) . . . . .	337
Configuring PIM Sparse Mode (NSM Procedure) . . . . .	339
Configuring a Rendezvous Point to Group Mappings (NSM Procedure) . . . . .	340
Configuring Acceptable Groups (NSM Procedure) . . . . .	341
Example: Configuring Proxy RP . . . . .	342
Multicast Routing Table Entries Overview . . . . .	344
Multicast Routing Table Preferences Overview . . . . .	344
Configuring Multicast Static Routes . . . . .	345
Example: Configuring Multicast Static Routes (NSM Procedure) . . . . .	345
IRDP Support Overview . . . . .	346
Example: Configuring ICMP Router Discovery Protocol (NSM Procedure) . . . . .	347
Disabling IRDP . . . . .	348
Policy-Based Routing Overview . . . . .	349
Example: Configuring Policy-Based Routing (NSM Procedure) . . . . .	349
<b>Chapter 11 Virtual Systems . . . . .</b>	<b>353</b>
Vsys DHCP Enhancement Overview . . . . .	353
Vsys Limitations Overview . . . . .	354
Example: Configuring Vsys Resource Limits (NSM Procedure) . . . . .	355
Vsys Session Limit Overview . . . . .	356
Example: Configuring Vsys Session Limit (NSM Procedure) . . . . .	356
Vsys CPU Limit Overview . . . . .	357

	Example: Configuring CPU Limit (NSM Procedure) . . . . .	358
<b>Chapter 12</b>	<b>User Authentication . . . . .</b>	<b>359</b>
	IEEE 802.1x Support Overview . . . . .	359
	Supported EAP Types . . . . .	360
<b>Chapter 13</b>	<b>High Availability . . . . .</b>	<b>361</b>
	NSRP Clusters Overview . . . . .	361
	Creating an NSRP Cluster . . . . .	363
	Configuring Active/Passive Cluster . . . . .	364
	Example: Configuring Active/Passive Cluster (NSM Procedure) . . . . .	365
	Active/Active Configurations Overview . . . . .	368
	Configuring an Active/Active Cluster (NSM Procedure) . . . . .	369
	Synchronizing Virtual Router Configurations and RunTime Objects (NSM Procedure) . . . . .	369
	Synchronizing Virtual Router Configurations . . . . .	370
	Configuring the Virtual Router Synchronization Settings . . . . .	370
	Synchronizing Runtime Objects . . . . .	371
	Changing VSD Group Member States (NSM Procedure) . . . . .	371
	Example: Changing VSD Group Member States (NSM Procedure) . . . . .	372
	Configuring NSRP to Detect Interface and Zone Failure . . . . .	373
	Configuring Track IPs . . . . .	374
	Configuring Interface Monitoring . . . . .	375
	Configuring Zone Monitoring . . . . .	375
	Configuring Monitor Threshold . . . . .	376
	Vsys Clusters Overview . . . . .	376
	Exporting and Importing Device Configurations (NSM Procedure) . . . . .	377
<b>Chapter 14</b>	<b>WAN, ADSL, Dial, and Wireless . . . . .</b>	<b>379</b>
	Wireless Settings in a Security Device Overview . . . . .	379
	Configuring General Wireless Settings . . . . .	380
	Configuring Antennas . . . . .	381
	Configuring Channels . . . . .	381
	Configuring Operation Mode Settings . . . . .	382
	Configuring Transmission Settings . . . . .	382
	Configuring Advanced Wireless Settings . . . . .	383
	Configuring Aging . . . . .	383
	Configuring Beacons . . . . .	384
	Configuring Burst and Fragment Size . . . . .	384
	Configuring Control Frame Protection . . . . .	385
	Configuring Short Slots . . . . .	386
	Configuring Preambles . . . . .	386
	Configuring Wireless MAC Access Lists . . . . .	387
	Configuring MAC Access Mode . . . . .	387
	Configuring MAC Addresses . . . . .	387
	Configuring Wireless General SSID Settings . . . . .	388
	Configuring SSID Authentication and Encryption . . . . .	389
	Configuring Wired Equivalent Privacy . . . . .	390
	Configuring WEP Keys . . . . .	391

	Using Wi-Fi Protected Access . . . . .	393
	Reactivating Wireless Connections . . . . .	394
	Conducting a Site Survey for Detecting Access Points . . . . .	395
	Network, Interface, and Security Modules Supported in Security Devices . . . . .	395
	Configuring the Network Module . . . . .	396
	Slot Information in Security Devices . . . . .	396
	Physical Interface Modules Supported by SSG520 and SSG550 Security Devices . . . . .	396
	Interface Modules (Copper) . . . . .	397
	10/100 Mbps . . . . .	397
	10/100/1000 Mbps . . . . .	397
	Interface Modules (Fiber) . . . . .	397
	Secure Port Modules . . . . .	398
	Chassis Information Overview . . . . .	399
	WPA2, Extended Range, and Super G Support on NetScreen5GT Wireless Overview . . . . .	399
	Wi-Fi Protected Access Overview . . . . .	400
	Configuring Wi-Fi Protected Access (NSM Procedure) . . . . .	400
	Super G Methods Overview . . . . .	402
	Configuring Atheros XR (NSM Procedure) . . . . .	402
<b>Chapter 15</b>	<b>General Packet Radio Service . . . . .</b>	<b>405</b>
	3GPP R6 Information Elements Support Overview . . . . .	405
	Radio Access Technology . . . . .	406
	Routing Area Identity and User Location Information . . . . .	406
	APN Restriction . . . . .	406
	IMSI Prefix Filtering . . . . .	406
	IMEI-SV . . . . .	406
	Configuring Access Point Name Restriction (NSM Procedure) . . . . .	407
	Configuring IMSI Prefix Filter (NSM Procedure) . . . . .	407
	DHCP Relay Overview . . . . .	408
<b>Part 2</b>	<b>Index</b>	
	Index . . . . .	411

# About This Guide

- [Objectives on page xv](#)
- [Audience on page xv](#)
- [Conventions on page xv](#)
- [Documentation on page xvii](#)
- [Requesting Technical Support on page xviii](#)

## Objectives

---

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

NSM 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, NSM enhances the overall security of the Internet gateway.

This guide explains how to configure NSM ScreenOS devices. For detailed NSM IDP device configuration, see the *Configuring Intrusion Detection and Prevention Devices Guide*. Use this guide in conjunction with the Network and Security Manager Administration Guide, Network and Security Manager Installation Guide, and Network and Security Manager Online Help.

## Audience

---

This guide is intended for system administrators 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

---

The sample screens used throughout this guide are representations of the screens that appear when you install and configure the NSM software. The actual screens may differ.

All examples show default file paths. If you do not accept the installation defaults, your paths will vary from the examples.

Table 1 on page xvi defines notice icons used in this guide.

Table 1: Notice Icons







Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page xvi defines text conventions used in this guide.

Table 2: Text Conventions

Convention	Description	Examples
<b>Bold typeface</b>	<ul style="list-style-type: none"> <li>Represents commands and keywords in text.</li> <li>Represents keywords</li> <li>Represents UI elements</li> </ul>	<ul style="list-style-type: none"> <li>Issue the <b>clock source</b> command.</li> <li>Specify the keyword <b>exp-msg</b>.</li> <li>Click <b>User Objects</b></li> </ul>
<b>Bold sans serif typeface</b>	Represents text that the user must type.	<b>user input</b>
<b>fixed-width font</b>	Represents information as displayed on the terminal screen.	<pre>host1# show ip ospf Routing Process OSPF 2 with Router ID 5.5.0.250 Router is an area Border Router (ABR)</pre>
Key names linked with a plus (+) sign	Indicates that you must press two or more keys simultaneously.	Ctrl + d



Table 2: Text Conventions (*continued*)

Convention	Description	Examples
<i>Italics</i>	<ul style="list-style-type: none"> <li>Emphasizes words</li> <li>Identifies variables</li> <li>Identifies chapter, appendix, and book names</li> </ul>	<ul style="list-style-type: none"> <li>The product supports two levels of access, <i>user</i> and <i>privileged</i>.</li> <li><i>clusterID</i>, <i>ipAddress</i>.</li> <li><i>Appendix A, System Specifications</i>.</li> </ul>
The angle bracket (>)	Indicates navigation paths through the UI by clicking menu options and links.	<b>Object Manager &gt; User Objects &gt; Local Objects</b>

Table 3 on page xvii defines syntax conventions used in this guide.

Table 3: Syntax Conventions

Convention	Description	Examples
Words in plain text	Represent keywords	terminal length
Words in italics	Represent variables	<i>mask</i> , <i>accessListName</i>
Words separated by the pipe (   ) symbol	Represent a choice to select one keyword or variable to the left or right of this symbol. The keyword or variable can be optional or required.	diagnostic   line
Words enclosed in brackets ( [ ] )	Represent optional keywords or variables.	[ internal   external ]
Words enclosed in brackets followed by and asterisk ( [ ]*)	Represent optional keywords or variables that can be entered more than once.	[ level1   level2   11 ]*
Words enclosed in braces ( { } )	Represent required keywords or variables.	{ permit   deny } { in   out } { clusterId   ipAddress }

## Documentation

Table 4 on page xvii describes documentation for the NSM.

Table 4: Network and Security Manager Publications

Book	Description
<i>Network and Security Manager Installation Guide</i>	Details the steps to install the NSM management system on a single server or on separate servers. It also includes information on how to install and run the NSM user interface. This guide is intended for IT administrators responsible for the installation and/or upgrade to NSM.

Table 4: Network and Security Manager Publications (*continued*)

Book	Description
<i>Network and Security Manager Administration Guide</i>	<p>describes how to use and configure key management features in the NSM. It provides conceptual information, suggested workflows, and examples where applicable. This guide is best used in conjunction with the Network and Security Manager Online Help, which provides step-by-step instructions for performing management tasks in the NSM UI.</p> <p>This guide is intended for application administrators or those individuals responsible for owning 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.</p>
<i>Network and Security Manager ScreenOS and IDP Devices Guide</i>	Describes NSM features that relate to device configuration and management. It also explains how to configure basic and advanced NSM functionality, including deploying new device configurations, managing Security Policies and VPNs, and general device administration.
<i>Network and Security Manager Online Help</i>	Provides task-oriented procedures describing how to perform basic tasks in the NSM user interface. It also includes a brief overview of the NSM system and a description of the GUI elements.
<i>Network and Security Manager API Guide</i>	Provides complete syntax and description of the SOAP messaging interface to the Network and Security Manager.
<i>Network and Security Manager Release Notes</i>	<p>Provides the 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.</p> <p>Release notes are included on the corresponding software CD and are available on the Juniper Networks Website. The documentation is also available on the Internet. You can order a set of printed documents from your Juniper Networks sales representative.</p>

## Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need postsales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.

- JTAC Hours of Operation —The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

### Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://www.juniper.net/alerts/>
- Join and participate in the Juniper Networks Community Forum: <http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Manager: <http://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool located at <https://tools.juniper.net/SerialNumberEntitlementSearch/>.

### Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Manager tool in the CSC at <http://www.juniper.net/cm/> .
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, visit us at <http://www.juniper.net/support/requesting-support.html>.



## PART 1

# Configuring

- [NSM User Interface and NSM Key Management Features on page 3](#)
- [Device Configuration on page 25](#)
- [Network Settings on page 37](#)
- [Advanced Network Settings on page 111](#)
- [Administration on page 145](#)
- [Security on page 173](#)
- [Planning and Preparing VPNs on page 193](#)
- [Configuring VPNs on page 217](#)
- [Voice Over Internet Protocol on page 277](#)
- [Routing on page 291](#)
- [Virtual Systems on page 353](#)
- [User Authentication on page 359](#)
- [High Availability on page 361](#)
- [WAN, ADSL, Dial, and Wireless on page 379](#)
- [General Packet Radio Service on page 405](#)



## CHAPTER 1

# NSM User Interface and NSM Key Management Features

Juniper Network and Security Manager (NSM) provides IT departments with an easy-to-use solution that controls all aspects of the Juniper Networks firewall, VPN, and IDP devices including device configuration, network settings, and security policy. NSM enables IT departments to control the entire device lifecycle with a single, centralized solution. Using NSM, you can configure all your Juniper Networks security devices from one location, at one time.

For details on ScreenOS functionality, see the *Concepts & Examples ScreenOS Reference Guide*.

This chapter contains the following topics:

- [NSM Overview on page 4](#)
- [Security Integration Management Using NSM Overview on page 4](#)
- [Managing Devices in a Virtual Environment Using NSM on page 6](#)
- [Error Prevention, Recovery, and Audit Management Using NSM on page 8](#)
- [Administering ScreenOS Devices Using NSM Complete System Management on page 10](#)
- [NSM User Interface Overview on page 12](#)
- [Understanding NSM User Interface Menus and Toolbars on page 12](#)
- [Working with Multiple NSM Administrators Overview on page 13](#)
- [NSM Modules Overview on page 13](#)
- [Investigate Task Modules in the NSM User Interface Overview on page 14](#)
- [Configure Task Modules in the NSM User Interface Overview on page 16](#)
- [Administer Task Modules in the NSM User Interface Overview on page 20](#)
- [Understanding Validation Icons and Validation Data in the NSM User Interface on page 21](#)
- [Understanding the Search Function in the NSM User Interface on page 22](#)

## NSM Overview

---

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 NSM, 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.

NSM 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.

NSM 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.

### Related Documentation

- [NSM User Interface Overview on page 12](#)
- [NSM Modules Overview on page 13](#)
- [Understanding NSM User Interface Menus and Toolbars on page 12](#)

## Security Integration Management Using NSM Overview

---

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 NSM, this location is the NSM GUI, 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.

The following topics are the security integration management features of NSM:

- [Complete Support on page 4](#)
- [Network Organization on page 5](#)
- [Role-Based Administration on page 5](#)
- [Centralized Device Configuration on page 5](#)
- [Migration Tools on page 6](#)

### Complete Support

You can create and manage device configurations for security devices or systems. NSM 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

With NSM, you can 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, and then create subdomains that automatically inherit these definitions from the global domain.

## Role-Based Administration

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

Use NSM 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 NSM 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 NSM as the super administrator, you have full access to all functionality within the global domain. From the global domain, you can add the following NSM 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 NSM system, and a role is a collection of activities that defines an administrative function. Use activities to create custom roles for your NSM administrators.
- **Administrators**—An administrator is a user of NSM 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.

## Centralized Device Configuration

No network is too large—because you manage your security devices from one location, you can use the following 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 reuse specific information. Create a device template that defines specific configuration values, and 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). In addition, you can make global-domain templates available for reference in subdomains.
- **Shared Objects**—An object is an NSM 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. Although, 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 NSM migration tools to quickly import your existing security devices and their configurations, address books, service objects, policies, VPNs, and administrator privileges. As NSM 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, NSM automatically transfers your existing domain structure.

For details on migrating from a previous management system, see the *NSM Migration Guide*.

### Related Documentation

- [Administering ScreenOS Devices Using NSM Complete System Management on page 10](#)
- [Managing Devices in a Virtual Environment Using NSM on page 6](#)
- [Error Prevention, Recovery, and Audit Management Using NSM on page 8](#)

---

## Managing Devices in a Virtual Environment Using NSM

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. NSM helps you take control of your network by providing a virtual environment in which to first model, verify, and then update your managed devices with changes.

The following topics are the device management features in NSM:

- [Device Modeling on page 7](#)
- [Rapid Deployment \(RD\) on page 7](#)
- [Policy-Based Management on page 7](#)

## 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. NSM includes configuration validation to help you identify device configuration errors and missing information, and 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 NSM, you can implement a new routing protocol across your network, design and deploy a new security policy with traffic shaping, or create a VPN tunnel that connects a branch office to your corporate network—then deploy all changes with a single click.

## Rapid Deployment (RD)

Rapid Deployment enables deployment of multiple security devices in a large networked environment with minimal user involvement. Rapid Deployment 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 Rapid Deployment, the NSM administrator creates a small file (called a configlet) in NSM, and then sends that configlet to an onsite administrator that has local access to the security device. With the help of the Rapid Deployment wizard, the onsite administrator installs the configlet on the device, which automatically contacts NSM and establishes a secure connection for device management.

Rapid Deployment is ideal for quickly bringing new security devices under NSM management for initial configuration. You can model and verify your device configurations for undeployed devices, and then install the completed device configuration when the device contacts NSM.

## Policy-Based Management

You can create simplified and efficient security policies for your managed devices using the Policy-Based Management feature. [Table 5 on page 8](#) describes the different policy-based management features:

Table 5: Policy-Based Management Options

Option	Description
Groups	Group your devices by platform, ScreenOS version, location, or function, and then add them to your security policies.
Zone Exceptions	Simplify your rules, by defining a common To Zone and From Zone for all devices in the rule, and 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 only).
Traffic Shaping	Use your firewall rules to control the amount of traffic permitted through your security devices.

**Related  
Documentation**

- [Device Configuration Settings Overview on page 25](#)
- [Working with Multiple NSM Administrators Overview on page 13](#)
- [Administering ScreenOS Devices Using NSM Complete System Management on page 10](#)

## Error Prevention, Recovery, and Audit Management Using NSM

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 NSM's error prevention and recovery features, you can ensure that you are consistently sending stable configurations to your devices, and that your device remains connected to NSM. Additionally, you can track each change made by an NSM administrator to help you identify when, how, and what changes were made to your managed devices.

The following topics are the error prevention, recovery, and audit management features in NSM:

- [Device Configuration Validation on page 9](#)
- [Policy Validation on page 9](#)
- [Atomic Configuration and Updating on page 9](#)
- [Device Image Updates on page 9](#)
- [Auditing on page 9](#)

## Device Configuration Validation

NSM automatically alerts you to configuration errors while you work in the UI. Each field that has incorrect or incomplete data displays a icon— move your mouse cursor over the icon to get details on the missing data. For more details on validation, see [“Understanding Validation Icons and Validation Data in the NSM User Interface”](#) on page 21.

## Policy Validation

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

## Atomic Configuration and Updating

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

Devices running ScreenOS 5.1 and later 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 the management connection from the NSM 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. The image updates are as follows:

- NSM updates—Use NSM to upload the new image file to multiple security devices with a single click.
- RMA updates—Replace failed devices, by setting the device to the RMA state, which enables NSM 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 will 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 it includes:

- Date and time the administrative action occurred
- NSM 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.

**Related  
Documentation**

- [Administering ScreenOS Devices Using NSM Complete System Management on page 10](#)
- [Security Integration Management Using NSM Overview on page 4](#)
- [Managing Devices in a Virtual Environment Using NSM on page 6](#)

---

## Administering ScreenOS Devices Using NSM Complete System Management

NSM provides the tools and features you need to manage your devices as a complete system, as well as individual networks and devices. The following features are supported in administering ScreenOS 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 NetScreen Redundancy Protocol (NSRP).

The following topics describe about how to administer ScreenOS devices using the complete system management feature in NSM:

- [VPN Abstraction on page 10](#)
- [Integrated Logging and Reporting on page 11](#)
- [Monitoring Status on page 11](#)
- [Job Management on page 11](#)

### 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, and 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 route-based VPNs to control traffic flow.
- Policy-based VPNs—Connect devices, remote access server (RAS) users, and control traffic flow (traffic flow can also be controlled using L2TP VPNs).

- 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 intrusions, and to record security events so you can monitor the important activities occurring on your network. You can use NSM to monitor, log, and report on network activity in *real-time* to help you understand what is happening on your network. For example, you can:

- 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

NSM keeps you up-to-date on the health of your network. You can view the following monitoring statuses on 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 redundant devices status in the NSRP Monitor.
- View the status of your IDP clusters in the IDP Cluster Monitor.
- View the health of the NSM 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. NSM 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, NSM 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 the following:

- 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.

**Related Documentation**

- [NSM Modules Overview on page 13](#)
- [Error Prevention, Recovery, and Audit Management Using NSM on page 8](#)
- [Device Configuration Settings Overview on page 25](#)

---

## NSM User Interface Overview

The NSM user interface (UI) is used to control the NSM system. Using the UI, you can configure NSM administrators, add devices, edit policies, and view reports—access the full functionality of the NSM system.



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

---

## Configuring UI Preferences

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

**Related Documentation**

- [NSM Modules Overview on page 13](#)
- [Understanding NSM User Interface Menus and Toolbars on page 12](#)
- [Understanding the Search Function in the NSM User Interface on page 22](#)

---

## Understanding NSM User Interface Menus and Toolbars

The NSM user interface (UI) appears after you log in, and it 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.

**Related Documentation**

- [NSM Modules Overview on page 13](#)
- [Understanding the Search Function in the NSM User Interface on page 22](#)



- [Understanding Validation Icons and Validation Data in the NSM User Interface on page 21](#)

## Working with Multiple NSM Administrators Overview

---

When multiple NSM administrators are accessing the NSM system at the same time, NSM ensures that all edits are synchronized by locking an active object. Only one administrator at a time can edit existing values for an object, but multiple administrators can still view the existing values for that object.

NSM administrators must know the following guidelines:

- When an NSM administrator begins editing an object, the UI locks that object to prevent other administrators from editing the object's value.
- During lockout, NSM makes "lazy" saves of all edits made and stores them in an in-memory database. If NSM crashes during a lazy save, edits made since the last lazy save are lost, and NSM prompts the NSM administrator to roll back to the last lazy save.
- When the NSM administrator completes and saves the edit, that object is unlocked, enabling other administrators 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 NSM administrator who is currently editing the object. Depending on your administrator privileges, you can locate contact information for the administrator 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 the *Network and Security Manager Administration Guide*.

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

### Related Documentation

- [NSM Modules Overview on page 13](#)
- [Device Configuration Settings Overview on page 25](#)

## NSM Modules Overview

---

The navigation tree contains 11 top-level modules that contain specific NSM functionality, as detailed in the following topics. There are three containers in the left UI pane that contains the 11 modules. They are Investigate, Configure, and Administer.

- [Navigation Tree on page 14](#)
- [Main Display Area on page 14](#)

## Navigation Tree

The navigation tree displays the 11 NSM modules in the left pane of the NSM window. Double-click a module to display its contents in a hierarchical tree format. For details about each module, see the [“NSM Modules Overview” on page 13](#).

## Main Display Area

The main display area displays content for the selected module or module contents. They are as follows:

- **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 *Network and 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.

### Related Documentation

- [NSM User Interface Overview on page 12](#)
- [Understanding NSM User Interface Menus and Toolbars on page 12](#)
- [Working with Multiple NSM Administrators Overview on page 13](#)

---

## Investigate Task Modules in the NSM User Interface Overview

The Investigate task includes the following top-level modules:

- [Log Viewer on page 14](#)
- [Report Manager on page 15](#)
- [Log Investigator on page 15](#)
- [Realtime Monitor on page 15](#)
- [Security Monitor on page 16](#)
- [Audit Log Viewer on page 16](#)

## 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 the *Network and Security Manager Administration Guide*.

## Report Manager

The Report Manager contains summary, graphs, and charts that detail specific security events that occur on your network. NSM 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 NSM. 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

## Realtime Monitor

Realtime Monitor provides a graphical view of the current status of all devices managed by NSM. [Table 6 on page 15](#) describes the monitoring status of all NSM managed devices.

**Table 6: Monitoring Status of NSM Managed Devices**

NSM Managed Devices	Monitoring Status
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 “Realtime Monitoring” in the *Network and Security Manager Administration Guide*.

## 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” in the *Network and Security Manager Administration Guide*.

## Audit Log Viewer

The Audit Log Viewer contains a log entry for every change made by an NSM administrator. For more details on Audit Log Viewer, see “Using the Audit Log Viewer” in the *Network and Security Manager Administration Guide*.

### Related Documentation

- [Configure Task Modules in the NSM User Interface Overview on page 16](#)
- [Administer Task Modules in the NSM User Interface Overview on page 20](#)
- [NSM Modules Overview on page 13](#)

## Configure Task Modules in the NSM User Interface Overview

The Configure task includes the following top-level modules:

- [Device Manager on page 16](#)
- [Security Policies on page 17](#)
- [VPN Manager on page 17](#)
- [Object Manager on page 18](#)

## Device Manager

The Device Manager contains the device objects that represent your security devices. [Table 7 on page 16](#) describes the objects that you can create in Device Manager.

**Table 7: Device Objects in Device Manager**

Device Object	Description
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 a vsys device that has a cluster as its root device.

Table 7: Device Objects in Device Manager (*continued*)

Device Object	Description
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 once and then use for multiple devices.
Device Groups	A device group is a user-defined collection of devices.

## Security Policies

Security policies contain 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 policies based on existing policies
- Install policies on one or multiple security devices
- Delete policies



**NOTE:** Devices running ScreenOS 6.3, support IPv6 in policy rulebases, IDP, address objects, and attack objects. You can also configure IPv6 host, network, and multicast addresses. For more information on IPv6 support, see the *Network and Security Manager Administration Guide*.

If the device configurations that you imported from your security devices contained policies, security policies display those imported policies. For details on editing those imported policies or creating policies, see Chapter 9, “Configuring Security Policies”, or Chapter 10, “Configuring VPNs”, of the *Network and Security Manager Administration Guide*.

## 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 Pproposals, 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.



**NOTE:** In ScreenOS 6.1 or later, users can set “group 14” for 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 server (RAS) and include multiple users.



**NOTE:** In ScreenOS 6.1 or later, AutoKey IKE VPN and AutoKey IKE RAS VPN are supported in IKEv2 parameters.

## Object Manager

The Object Manager contains objects, which are reusable, basic NSM 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.

Table 8 on page 18 describes the objects that you can create in NSM.

**Table 8: Objects in Object Manager**

Objects	Description
Address Objects	Represent components of your network (hosts, networks, servers). On devices running ScreenOS 6.3, the new policy appears in the security policy list and supports IPv6 in policy rule bases, IDP, address and attack objects. After you have created a security policy, you can add rules to the new policy. Rules include IPv4, IPv6, VPN, and also VPN link. For more information, see the <i>IDP Concepts &amp; Examples guide</i> . A rule with combination of IPv4 or IPv6 address objects is not allowed.
QoS Profiles	Represent the resource reservation control mechanisms rather than the achieved service quality. You can provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow. You can configure QoS into a policy role, using role options. There are two types of QoS profiles and they are DSCP and IP precedence.
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 Objects	Define the attack signature patterns, protocol anomalies, and the action you want a security device to take against matching traffic. On devices running ScreenOS 6.3, you can also set IPv6 version signature information while editing IP settings and header matches of a custom attack.

Table 8: Objects in Object Manager (*continued*)

Objects	Description
IDP Attack Objects	Represent attack patterns that detect known and unknown attacks. You use IDP attack objects within IDP rules. On devices running ScreenOS 6.3, you can also set IPv6 version signature information while editing IP settings and header matches of a custom attack. When you select the IPv6 option, the Protocol tab displays the ICMP6 Packet Header Fields value, and then you can also modify the respective configurable parameters.
AV Objects	Represent the AV servers, software, and profiles available to devices managed by NSM.
ICAP Objects	Represent 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. NSM contains a database of Service Objects for well-known services; you can also create Service Objects to represent the custom services you are running on your network.
SCTP Objects	<p>Provide a reliable transport service that supports data transfer across the network, in sequence and without errors. s of ScreenOS 6.3, the existing SCTP stateful firewall supports protocol filtering.</p> <p><b>NOTE:</b> You can configure the security device to perform stateful inspection on all SCTP traffic without performing deep inspection (DI). If you enable stateful inspection of SCTP traffic, the SCTP ALG drops any anomalous SCTP packets.</p>
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, and 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 SecureID servers. You can use an authentication server object to authenticate NSM administrators (RADIUS only), XAuth users, IKE RAS users, L2TP users, and IKEv2 EAP users. NSM provides configuration support for Authentication Manager version 5 or later. This provision has introduced the concept of a primary server with up to 10 replica servers. In the Primary/Replica version, each server can process authentication requests. The more current agents will send to the server, the faster the responder.
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.

Table 8: Objects in Object Manager (*continued*)

Objects	Description
CRL Objects	Represent the certificate authority's certificate revocation list.
<p>You can use the object Manager to:</p> <ul style="list-style-type: none"> <li>• View and/or edit the object properties</li> <li>• Create, edit, or delete objects</li> <li>• Create custom groups of Objects</li> </ul> <p>For more details on objects, see Chapter 8, “Configuring Objects,” of the <i>Network and Security Manager Administration Guide</i>.</p>	
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Investigate Task Modules in the NSM User Interface Overview on page 14</a></li> <li>• <a href="#">Administer Task Modules in the NSM User Interface Overview on page 20</a></li> <li>• <a href="#">NSM Modules Overview on page 13</a></li> </ul>

## Administer Task Modules in the NSM User Interface Overview

The Administer task includes the following top-level modules:

- [Server Manager on page 20](#)
- [Job Manager on page 20](#)
- [Action Manager on page 20](#)

### 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 NSM system.

### Job Manager

Job Manager contains the status of commands (also called directives) that NSM 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” in the *Network and Security Manager Administration Guide*.

### 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” in the *Network and Security Manager Administration Guide*.

**Related Documentation**

- [Investigate Task Modules in the NSM User Interface Overview on page 14](#)
- [Configure Task Modules in the NSM User Interface Overview on page 16](#)



- [NSM Modules Overview on page 13](#)

## Understanding Validation Icons and Validation Data in the NSM User Interface

NSM uses automatic validation to help you identify the integrity of a configuration or specific parameter at a glance. Validation and data origination icons show the user where field data originates. These are implemented as additional types of validation messages (beyond the current error and warning messages), including Template Value, Override, and From Object messages. Each has its own icon and text color in the tool tips. [Table 9 on page 21](#) lists the validation signs and validation and data origination icons that may appear as you work in the UI.

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.

**Table 9: Validation Status, Validation, and Data Origination Icons for ScreenOS Devices**

Validation Status and Icons	Description
<b>Validation Status</b>	
Error	Indicates that a configuration or parameter is not configured correctly in the NSM UI. Updating a device with this modeled configuration causes problems on the device. This is the highest priority validation icon.
Warning	Indicates that a configuration or parameter is not configured correctly in the NSM UI. Updating a device with this modeled configuration might cause problems on the device.
Needs Validation	Indicates that a configuration or parameter has not been validated. Although NSM 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.
Valid	Indicates that a configuration or parameter is configured correctly in the NSM UI.
<b>Validation and Data Origination Icons</b>	
Override	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-provided value.
Template Value	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.
From Object	Indicates that the displayed value came from the device when the device was imported. Changes to a template will not change this value unless you selected <b>Remove conflicted device values</b> in the template Operations dialog box. This is the lowest priority validation and data origination icon.

- Related Documentation**
- [Understanding NSM User Interface Menus and Toolbars on page 12](#)
  - [Understanding the Search Function in the NSM User Interface on page 22](#)
  - [NSM Modules Overview on page 13](#)

## Understanding the Search Function in the NSM User Interface

You can use the integrated search feature in NSM 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.

Press the key that represents the search mode you want to use, and then begin entering the search criteria. Switching to another view or pressing the ESC key ends the search operation and closes the tool window. [Table 10 on page 22](#) describes the detail sections in each search mode.

**Table 10: Search Functions in the NSM UI**

Search Mode	Function	Your Action
Contains String [C] Search Mode	Use to locate a pattern anywhere in a string.	<p>For example, to locate the pattern "RPC" in service objects:</p> <ol style="list-style-type: none"> <li>1. In the NSM navigation tree, select <b>Object Manager &gt; Service Objects &gt; Predefined Service Objects</b>, and then select the Service Object icon at the top of the Service Tree tab.</li> <li>2. Enter <b>C</b>, and then enter <b>RPC</b>. The UI automatically highlights the first match, MS-RPC-ANY.</li> </ol>
Starts with [S] Search Mode	Use to locate a pattern at the beginning of a string.	<p>For example, to locate the pattern "OR" in security devices:</p> <ol style="list-style-type: none"> <li>1. In the NSM navigation tree, select <b>Device Manager &gt; Devices &gt; Predefined Service Objects</b>, then select the Service Object icon at the top of the Device Tree tab.</li> <li>2. Enter <b>S</b>, then enter <b>OR</b>. The UI automatically highlights the first match, OR_EU_208.</li> </ol>

Table 10: Search Functions in the NSM UI (*continued*)

Search Mode	Function	Your Action
Regular Expression [R] Search Mode	Use to locate a value using a regular expression.	<p>For example, to locate all attack objects that detect denial-of-service attacks:</p> <ol style="list-style-type: none"> <li>1. In the NSM navigation tree, select <b>Object Manager &gt; Attack Objects</b>, and then select the <b>Predefined Attacks</b> tab.</li> <li>2. Select the first entry in the Name column, and then press the backslash key (\) to display the search mode window.</li> <li>3. Enter <b>R</b>, and then enter the following characters: <b>DoS .enial</b>.</li> </ol> <p>The UI automatically highlights the first match; click the Down Arrow key to highlight the next match.</p> <p><b>NOTE:</b> The regular expression search mode supports all common regular expressions. For more information about regular expressions, refer to a dedicated resource, such as <i>Mastering Regular Expressions, 2nd Edition</i>, by Jeffrey E. F. Friedl.</p>
IP [I] Search Mode	Use to locate an IP address.	<p>For example, to locate the IP address 5.5.5.50 and 5.5.5.51 in Address Objects:</p> <ol style="list-style-type: none"> <li>1. In the NSM navigation tree, select <b>Object Manager &gt; Address Objects</b>, and then select the <b>Address Table</b> tab.</li> <li>2. Select the first entry in the Name column IP/Domain, and then press the backslash key (\) to display the search mode window.</li> <li>3. Enter <b>I</b>, and then enter <b>5.5.5.*</b>. The UI automatically highlights the first match, <b>5.5.5.50</b>. Click the Down Arrow key to highlight the next match, 5.5.5.51.</li> </ol>

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.

#### Related Documentation

- [Understanding Validation Icons and Validation Data in the NSM User Interface on page 21](#)
- [NSM Modules Overview on page 13](#)
- [NSM User Interface Overview on page 12](#)



## CHAPTER 2

# Device Configuration

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 NSM 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 a brief overview on how best to create your virtual network and simplify management tasks. For detailed information, see the *Network and Security Manager Administration Guide*.

This chapter contains the following topics:

- [Device Configuration Settings Overview on page 25](#)
- [Configuring Advanced Properties for ScreenOS Device Details on page 26](#)
- [Configuring a Blacklisted Entry \(NSM Procedure\) on page 27](#)
- [Enabling ALGs \(NSM Procedure\) on page 28](#)
- [Understanding Device Configurations Running ScreenOS 5.4 FIPS and Later Overview on page 29](#)
- [Configuring Extranet Devices Overview on page 30](#)
- [Configuring Extranet Devices Details \(NSM Procedure\) on page 30](#)
- [Understanding Templates and Groups on page 32](#)
- [Configuring Network Settings Options and Descriptions on page 34](#)

## Device Configuration Settings Overview

---

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 take effect.



**NOTE:** When you open a device for viewing or editing, the NSM 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.”

NSM 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 NSM 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 Extranet Devices

NSM also enables you to configure an existing extranet device (that is, a third-party router). You can do this by creating a script to perform the required actions on the extranet device.

Add the extranet device in the Device Manager, and then configure the required metadata in a shared object in the Object Manager under “Extranet Policies.” This data may include: credential information (user/password), IP address, 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.

### Related Documentation

- [Configuring Advanced Properties for ScreenOS Device Details on page 26](#)
- [Understanding Device Configurations Running ScreenOS 5.4 FIPS and Later Overview on page 29](#)
- [Understanding Templates and Groups on page 32](#)
- [Configuring Extranet Devices Details \(NSM Procedure\) on page 30](#)

---

## Configuring Advanced Properties for ScreenOS Device Details

When a denial-of-service (DoS) attack occurs, the CPU recognizes the attack and drops the traffic. A DoS attack can cause high CPU utilization and cause the security device to drop all packets. To prevent high CPU utilization during a DoS attack, the packet dropping feature was moved to the application-specific integrated circuit (ASIC) in ScreenOS 6.0.

Network traffic is categorized as critical and noncritical. Critical traffic includes management traffic such as Telnet and SSH. When a DoS attack occurs, CPU usage increases and when it reaches the throttling threshold, it triggers the dropping of noncritical traffic, which is not blacklisted. To prevent this, you can configure the security device to drop malicious packets within the device that processed them. In this mechanism, you create a blacklist with source and destination network addresses from which malicious traffic reaches the security device.

When a packet reaches the security device, the packets are checked against a list of configured blacklisted entries. If a match occurs, the device drops that packet. If the packet does not match the blacklisted entry, the device passes the packet to the next stage that prioritizes the packet. For each entry in the blacklist, the security device maintains a drop counter to record the number of packets dropped against that entry.

**Related Documentation**

- [Device Configuration Settings Overview on page 25](#)
- [Enabling ALGs \(NSM Procedure\) on page 28](#)
- [Understanding Device Configurations Running ScreenOS 5.4 FIPS and Later Overview on page 29](#)

## Configuring a Blacklisted Entry (NSM Procedure)

To configure a blacklisted entry:

1. In the NSM navigation tree, click **Device Manager > Devices**.
2. Select an ISG1000, ISG2000, NetScreen–5200, or NetScreen–5400 device.
3. Click the **Edit** icon to edit the device. The Device dialog box for the selected device appears.
4. In the device navigation tree, click **Advanced > CPU > Blacklist/Throttling Threshold**. Click the **Add** icon. The New Blacklist Entry dialog box appears.
5. Modify the settings as described in [Table 11 on page 27](#). Click **OK**.

**Table 11: Blacklist Configuration Fields**

Field	Description
ID	The ID of the blacklist is generated automatically.
Source IP	The source IP address from which the DoS attack traffic originated.
Destination IP	The destination IP address.
Source Port	The source port in a TCP or UDP session. Set this to 0 to match all ports.
Destination Port	The destination port in a TCP or UDP session. Set this to 0 to match all ports.

Table 11: Blacklist Configuration Fields (*continued*)

Field	Description
Protocol	The source port and destination port are valid only when you have set the protocol as UDP or TCP. Set this value to 0 to match any protocol.
Source IP Net Mask	The range is 0-32. Set this field to 0 to match all source IP addresses.
Destination IP Mask	The range is 0-32. Set this field to 0 to match all destination IP addresses.



**NOTE:** A blacklist with 0 timeout will not expire.

#### Related Documentation

- [Enabling ALGs \(NSM Procedure\) on page 28](#)
- [Configuring Extranet Devices Details \(NSM Procedure\) on page 30](#)
- [Configuring Network Settings Options and Descriptions on page 34](#)

## Enabling ALGs (NSM Procedure)

In ScreenOS 6.0, the following modifications were made to prevent high CPU utilization.

- Some existing Application Layer Gateways (ALGs) are disabled by default on high-end platforms (ISG1000, ISG2000, NetScreen 2000 line, and NetScreen line). The affected ALGs are H.323, SIP, MGCP, SCCP, MSRPC, SunRPC, and SQL. ALGs included in ScreenOS 6.1 are PAT for PPTP, SCTP, and Apple iChat. As of ScreenOS 6.3, the DNS Inhibit AAAA (IPv6) ALG is supported but disabled by default.
- ALGs included in ScreenOS 6.0 or later are enabled by default. They are FTP, DNS, Real, Rlogin, RSH, TALK, TFTP, and XING.

For efficient CPU utilization, you can enable or disable the ALGs.

To enable or disable the ALGs:

1. In the NSM navigation tree, click **Device Manager > Devices**.
2. Select a device or a model device
3. Click the **Edit** icon to edit the device. The relevant device dialog box appears.
4. In the device navigation tree, click **Advanced > ALGs**.
5. ALGs are listed depending on the type of device you selected and the OS version. ALGs can be enabled or disabled by checking or clearing their check boxes. See [Table 12 on page 29](#).



Table 12: ALGs Default Status

ALGs	Status
H.323, SIP, MGCP, SCCP, MSRPC, SunRPC, SQL, PPTP, and DNS Inhibit AAAA(IPv6).	Disabled by default on ISG1000, ISG2000, NetScreen-2000 line, and NetScreen-5000 line running ScreenOS 6.0 or later.
FTP, DNS, Real, Rlogin, RSH, TALK, TFTP, XING, and SCTP	Enabled by default on a device running ScreenOS 6.0 or later.

- Related Documentation**
- [Configuring Advanced Properties for ScreenOS Device Details on page 26](#)
  - [Configuring a Blacklisted Entry \(NSM Procedure\) on page 27](#)
  - [Device Configuration Settings Overview on page 25](#)

## Understanding Device Configurations Running ScreenOS 5.4 FIPS and Later Overview

The following features are disabled on security devices running the Federal Information Processing Standards (FIPS) certified release of ScreenOS (ScreenOS 5.4 FIPS):

- SNMP management
- MD5 algorithm
- Group 5 Phase 2 IKE proposals

For more information about FIPS-enabled security devices, refer to the ScreenOS 5.0 FIPS Reference Note.



**NOTE:** To configure and manage security devices running ScreenOS 5.0 FIPS using NSM, you must first configure a VPN tunnel between the device and the NSM GUI server. After establishing this tunnel, you cannot reconfigure tunnel parameters in NSM.

## About Configuring Devices Running Future Releases of ScreenOS

You can use NSM 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 that 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 cannot, 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 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.

**Related  
Documentation**

- [Device Configuration Settings Overview on page 25](#)
- [Configuring Network Settings Options and Descriptions on page 34](#)
- [Configuring Zones and Zone Properties in ScreenOS Devices Overview on page 39](#)

---

## Configuring Extranet Devices Overview

NSM also enables you to configure an existing extranet device (a 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, and then configure the required metadata in a shared object in the Object Manager under Extranet Policies. This data might include: credential information (user/password), IP address, 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.

**Related  
Documentation**

- [Configuring Extranet Devices Details \(NSM Procedure\) on page 30](#)
- [Configuring Network Settings Options and Descriptions on page 34](#)

---

## Configuring Extranet Devices Details (NSM Procedure)

This example shows how 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 NSM navigation tree, click **Object Manager > Custom Policy Fields**.
2. Select the **Field Definition** tab, and then click **New**. The New Custom Policy Fields Meta Data window appears.

### 3. Configure the Custom Policy Field:

- Enter a name for the field: enter **ID**.
- Click the **Required** check box.
- Select **Integer** from the Field Type list.
- Enter a value in the Validation String box.
- Enter any appropriate comments.
- Click **OK**. A folder for the ID custom policy field object appears.
- In the Objects tab, click on the ID folder. Click **New**. The New Custom Policy Fields Data window appears.
- Enter a value in the Data Value field: enter **1**. Click **OK**. The new value appears in the ID folder.
- 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 NSM navigation tree, click **Object Manager > Extranet Policies**. Then click **Add Policy** and the New ExtranetPolicyObject window appears.
2. Enter the name of the Extranet Policy: enter **Extranet Policy1**. Add a comment in the Comments field.
3. Configure the Extranet Policy object:
  - Click **Add Rule**. The New - Rule window appears.
  - 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 services in the Service tab.
  - Select the integer IDs that you created in the Custom Policy Field object in the Options tab.
4. 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, and then bind the extranet policy to the appropriate interface.

To create an Extranet Device:

1. In the NSM navigation tree, click **Device Manager > 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: enter **Cisco Router1**.
  - Select a color to represent the device.
  - Enter the IP address for the device.
  - Click **Show** in the Supplemental Data area. Additional fields appear, allowing you to configure supplemental information for the device, including the netmask, interfaces, and device root administrator.
  - Click the **Add** icon in the Interfaces field. The New Extranet Device Interface window appears.
  - Configure the interface. Enter a name for the interface, and add an IP address, and an interface mask. Then assign an extranet policy to it: for example, assign the Extranet Policy1 object you configured previously. Click **OK**.
  - Configure the device root administrator. Enter the administrator user name, and 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.

**Related  
Documentation**

- [Device Configuration Settings Overview on page 25](#)
- [Configuring Advanced Properties for ScreenOS Device Details on page 26](#)

---

## Understanding Templates and Groups

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.

When you apply a template to a device, NSM 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.



**NOTE:** For more information on using templates, template limitations, and exporting and importing device templates, see *Network and Security Manager Administration Guide*. For instructions on creating and applying templates, see the *Network and Security Manager Online Help* topics “Adding Device Templates” and “Applying Templates.”

- [Using Global Device Templates on page 33](#)
- [Using Device Groups on page 33](#)

## Using Global Device Templates

In NSM, you can make global-domain templates available for reference in subdomains. However, if an administrator disables the Allow use of global templates in subdomains flag in the preferences, the administrator must also identify and remove all uses of the global templates in the subdomains. You can do this by removing the template from subdomain devices with the template operations directive in each relevant subdomain.

## 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 NSM 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 NSM 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. For examples on creating a device group or configuring device information, see *Network and Security Manager Administration Guide*.

- Related Documentation**
- [Device Configuration Settings Overview on page 25](#)
  - [Configuring Advanced Properties for ScreenOS Device Details on page 26](#)
  - [NSM User Interface Overview on page 12](#)
  - [Understanding NSM User Interface Menus and Toolbars on page 12](#)

## Configuring Network Settings Options and Descriptions

The Network screens contain the options that enable the device to connect to and operate in the network. In the NSM navigation tree, click **Device Manager > Devices**, and then select a device. In the Device navigation tree, select **Network** to see the network settings options.

[Table 13 on page 34](#) describes the detailed configuration methods available for network settings.

**Table 13: Network Settings Options**

Network Settings Options	Description
<a href="#">"Vsys DHCP Enhancement Overview" on page 353</a>	This option is available only for NetScreen-5GT Wireless security devices running ScreenOS 5.0.0-WLAN; this device can act as a wireless access point (WAP). The wireless settings specify how the WAP connects multiple wireless networks or a wireless network to a wired network.
<a href="#">"Network, Interface, and Security Modules Supported in Security Devices" on page 395 (Slot and Chassis)</a>	This option is only available for security device systems, such as the NetScreen 5000 line, ISG1000, ISG2000, SSG520M, and SSG550M, that contain a motherboard or physical slots in which you can install optional modules. You can view or edit the type of network module installed in each available slot in the physical device.
<a href="#">"Configuring Virtual Routers" on page 292</a>	A virtual router (VR) supports static routes, dynamic routing protocols, and multicast protocols. The virtual router configuration includes the configuration for dynamic routing protocols and multicast protocols. As of ScreenOS 6.2, on high-end platforms you can change the management zone virtual router to an existing virtual router that is no longer bound to the trust-vr. The management zone virtual router supports out-of-band management and segregates firewall management traffic away from production traffic.
<a href="#">"Configuring Zones and Zone Properties in ScreenOS Devices Overview" on page 39</a>	A security zone is a specific network segment for which you can control inbound and outbound traffic. You can configure predefined zones or create user-defined security zones. You can also create a tunnel zone, which is a logical segment to which a VPN tunnel interface is bound.
<a href="#">"Interface Types in ScreenOS Devices Overview" on page 50</a>	You bind interfaces to predefined or user-defined security zones or to tunnel zones to permit traffic to pass into or out of the zone. For an interface in Route or NAT mode, you assign an IP address to the interface.
<a href="#">"Example: Configuring DIP Groups (NSM Procedure)" on page 100</a>	You can configure a range of IP addresses from which security device can take addresses when performing NAT on the source IP address of outgoing or incoming IP packets.
<a href="#">"About Configuring PPPoE" on page 135</a>	This option is only available for some security devices. You can configure PPPoE to enable the security device to connect to remote sites.

Table 13: Network Settings Options (*continued*)

Network Settings Options	Description
<a href="#">"Using the PPP Option to Configure Point-To-Point Protocol Connections" on page 134</a>	This option is only available for some security devices. You can configure PPP to enable the security device to connect to remote sites.
<a href="#">"Configuring a PPPoA Client Instance" on page 141</a>	On the ADSL interface (available on the NetScreen-5GT ADSL security device), you can configure a PPPoA client instance with a username, password, and other parameters, and then bind the instance to the ADSL interface (or subinterface) to enable Internet access for an internal network.
<a href="#">"Configuring a NetScreen Address Change Notification" on page 141</a>	This option is only available for security devices running ScreenOS 5.x. You configure NetScreen Address Change Notification to enable the security device to alert NSM of any change in the IP address assigned by a DHCP or PPPoE server.
<a href="#">"Interface Failover in ScreenOS Devices" on page 141</a>	This option is only available for some security devices. When there are both primary and backup interfaces to the Untrust zone, you can configure failover traffic from the primary to the backup interface, and from the backup to the primary interface.
<a href="#">"Example: Configuring Modem Connections (NSM Procedure)" on page 142</a>	This option is only available for some security devices. You can connect and configure an external modem to the RS-232 serial port as a backup dialup interface for traffic to the Untrust zone.
<a href="#">"DNS Server Configuration Using DNS Settings" on page 103</a>	Before the security device can use DNS for domain name and address resolution, you must configure the addresses for the primary and secondary DNS servers.
<a href="#">"Advanced Network Settings Overview" on page 108</a>	This option contains additional network settings you can configure.

**Related Documentation**

- [Configuring Zones and Zone Properties in ScreenOS Devices Overview on page 39](#)
- [Interface Types in ScreenOS Devices Overview on page 50](#)
- [Configuring Physical and Function Zone Interfaces in ScreenOS Devices Overview on page 52](#)
- [Interface Network Address Translation Using DIPs on page 67](#)





## CHAPTER 3

# Network Settings

The Device Manager module in Network and Security Manager (NSM) 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 the *Network and Security Manager Administration Guide*.

This chapter details the device configuration parameters, and provides configuration examples when possible. For instructions on configuring specific device settings, see the *Network and Security Manager Online Help*.

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 the *Network and Security Manager Administration Guide*.

Use security policies to configure firewall and VPN rules that control traffic on your network. Use the VPN Manager to configure VPNs.

- [Configuring Zones and Zone Properties in ScreenOS Devices Overview on page 39](#)
- [Predefined Screen Options Overview on page 40](#)
- [Configuring Flood Defense Settings for Preventing Attacks on page 41](#)
- [Example: Configuring UDP Flooding Protection \(NSM Procedure\) on page 43](#)
- [HTTP Components and MS-Windows Defense Method on page 43](#)
- [Protection Against Scans, Spoofs, and Sweeps on page 44](#)
- [IP and TCP/IP Anomaly Detection on page 45](#)
- [Prevention of Security Zones Using Denial of Service Attacks on page 47](#)
- [Malicious URL Protection on page 49](#)
- [Example: Enabling the Malicious URL Blocking Option \(NSM Procedure\) on page 50](#)
- [Interface Types in ScreenOS Devices Overview on page 50](#)
- [Configuring Physical and Function Zone Interfaces in ScreenOS Devices Overview on page 52](#)
- [Setting Interface Properties Using the General Properties Screen on page 53](#)
- [Setting WAN Properties Using the WAN Properties Screen on page 54](#)
- [Setting Port Properties Using the Port Properties Screen on page 54](#)

- [Using MLFR and MLPPP Options on page 55](#)
- [Setting Physical Link Attributes for Interfaces on page 55](#)
- [Enabling Management Service Options for Interfaces on page 56](#)
- [Setting DHCPv6 Overview on page 57](#)
- [Example: Assigning TCP/IP Settings for Hosts Using DHCP \(NSM Procedure\) on page 58](#)
- [Configuring Custom DHCP Options \(NSM Procedure\) on page 59](#)
- [Using Interface Protocol on page 61](#)
- [Using Interface Secondary IP on page 61](#)
- [Enabling ScreenOS Devices for Interface Monitoring on page 61](#)
- [Supporting Generic Routing Encapsulation Using Tunnel Interfaces on page 62](#)
- [Interface Network Address Translation Methods on page 62](#)
- [Interface Network Address Translation Using MIPs on page 62](#)
- [Example: Configuring MIPs \(NSM Procedure\) on page 63](#)
- [Interface Network Address Translation Using VIPs on page 65](#)
- [Mapping Predefined and Custom Services in a VIP on page 65](#)
- [Example: Configuring VIPs \(NSM Procedure\) on page 66](#)
- [Interface Network Address Translation Using DIPs on page 67](#)
- [Example: Enabling Multiple Hosts Using Port Address Translation \(NSM Procedure\) on page 68](#)
- [Example: Translating Source IP Addresses into a Different Subnet \(NSM Procedure\) on page 69](#)
- [Enabling Managed Devices Using Incoming DIP on page 73](#)
- [Example: Configuring Interface-Based DIP \(NSM Procedure\) on page 74](#)
- [Example: Configuring DIP Pools on the Untrust Interface \(NSM Procedure\) on page 75](#)
- [Example: Configuring an Aggregate Interface \(NSM Procedure\) on page 77](#)
- [Example: Configuring a Multilink Interface \(NSM Procedure\) on page 78](#)
- [Example: Configuring a Loopback Interface \(NSM Procedure\) on page 79](#)
- [Configuring Virtual Security Interfaces on page 80](#)
- [Example: Configuring a Redundant Interface \(NSM Procedure\) on page 80](#)
- [Example: Configuring a Subinterface \(NSM Procedure\) on page 84](#)
- [Example: Configuring a WAN Interface \(NSM Procedure\) on page 86](#)
- [Configuring a Tunnel Interface on page 87](#)
- [ADSL Interface in ScreenOS Devices on page 88](#)
- [ADSL, ADSL Interface, and ADSL Settings in ScreenOS Devices on page 89](#)
- [Determining Physical Ports and Logical Interfaces and Zones Using ScreenOS Devices Port Mode on page 91](#)
- [Backup Connection Using the Untrusted Ethernet Port in ScreenOS Devices on page 92](#)

- [Example: Configuring NetScreen5GT Devices to Permit Internal Hosts \(NSM Procedure\) on page 93](#)
- [Example: Configuring NetScreen5GT Devices to Connect to the Web Using the PPPoA and ADSL Interfaces \(NSM Procedure\) on page 94](#)
- [Example: Configuring NetScreen5GT Devices as a Firewall Using the PPPoE and ADSL Interfaces \(NSM Procedure\) on page 96](#)
- [Wireless Interface on ScreenOS Devices Overview on page 99](#)
- [Configuring DSCP Options Overview on page 99](#)
- [Example: Configuring DIP Groups \(NSM Procedure\) on page 100](#)
- [DNS Server Configuration Using DNS Settings on page 103](#)
- [Example: Configuring DNS Proxy Entries \(NSM Procedure\) on page 105](#)
- [Example: Configuring DDNS Settings \(NSM Procedure\) on page 106](#)
- [Advanced Network Settings Overview on page 108](#)

## Configuring Zones and Zone Properties in ScreenOS Devices Overview

The Zone screen is where you can configure predefined zones or create user-defined security zones. You can also create a tunnel zone, which is a logical segment to which a VPN tunnel interface is bound.

A security device supports two types of zones:

- Security zone—A Layer 3 security zone binds to NAT or Route mode interfaces; a Layer 2 security zone binds to Transparent mode interfaces.



**NOTE:** When you add a device and configure it to operate in Transparent mode, the L2 zone names appear in the NSM UI without the “V1-” prefix. When you update the configuration on the device from the UI, the correct L2 zone names are configured.

- Tunnel zone—A zone that binds to a carrier zone.

To add a zone to a security device, in the device navigation tree, select **Network > Zone** and add the desired zone. For Security Zones, you might define the name of the zone and the virtual router in which you want to place the zone; For tunnel zones, you must also specify the *carrier zone*, which is the security zone with which the tunnel zone is logically associated. A carrier zone provides firewall protection to the encapsulated traffic.

For more information about zones on security devices, refer to the *Concepts & Examples ScreenOS Reference Guide: Fundamentals*.

You can configure general properties and SCREEN attack protection for predefined or custom Security Zones.

### Zone General Properties

For predefined zones, some general properties are already configured for you, such as the Name and Virtual Router settings. For custom security zones, you can enter a name and select the virtual router that handles traffic to and from the new zone.

For both predefined and custom zones, you can configure the settings as described in [Table 14 on page 40](#).

**Table 14: Zone General Properties**

Custom Zone Settings	Description
TCP/IP Reassembly for ALG	Select this option when using Application Layer Gateway (ALG) filtering on the security device. By reassembling fragmented IP packets and TCP segments, the security device can accurately filter traffic.
Block Intrazone Traffic	Select this option to block traffic between hosts within the security zone.
TCP-RST	Select this option to return a TCP segment with the RESET flag set to 1 when a TCP segment with a flag other than SYN is received.
Asymmetric VPN	In asymmetrical encryption, one key in a pair is used to encrypt and the other to decrypt VPN traffic. When configuring multiple VPN tunnels to enable tunnel failover, enable this option for the Trust zones on each security device in the VPN so that if an existing session established on one VPN tunnel transfers to another, the security device at the other end of the tunnel does not reject it.

- Related Documentation**
- [Predefined Screen Options Overview on page 40](#)
  - [Interface Types in ScreenOS Devices Overview on page 50](#)
  - [Setting Interface Properties Using the General Properties Screen on page 53](#)

## Predefined Screen Options Overview

Typically, a network forwarding device such as a router or switch does not reassemble fragmented packets that it receives. It is the responsibility of the destination host to reconstruct the fragmented packets when they all arrive. Because the purpose of forwarding devices is the efficient delivery of traffic, queuing fragmented packets, reassembling them, refragmenting them, and then forwarding them is unnecessary and inefficient. However, passing fragmented packets through a firewall is insecure. An attacker can intentionally break up packets to conceal traffic strings that the firewall otherwise would detect and block.

You can enable predefined screen options that detect and block various kinds of traffic that the security device determines to be potentially harmful. To secure all connection attempts, security devices use a dynamic packet filtering method known as stateful inspection. Using this method, the device notes various components in a packet header, such as source and destination IP addresses, source and destination port numbers, and packet sequence numbers. The device uses this information to maintain the state of each session traversing the firewall.

A security device uses stateful inspection to secure a zone by inspecting, and then permitting or denying, all connection attempts that require crossing an interface from and to that zone. To protect against attacks from other zones, you can enable defense mechanisms known as screen attack protections, which detect and deflect TCP, UDP, IP, and ICMP packet attacks. Common screen attacks are SYN floods, packet fragments, and SYN and FIN bits set. When screen attack protections are enabled, the device generates a screen alarm log entry for each violation.

To configure Screen attack protections, open a device configuration and select **Network > Zone** to display the Zone configuration. Double-click a zone to display the Predefined Zone dialog box and select **SCREEN**.



**NOTE:** For instructions for configuring the SCREEN options, see the *Network and Security Manager Online Help* topic “Configuring SCREEN Options.” For information about the SCREEN alarm log entries that enabling these options can generate, see the *Network and Security Manager Administration Guide*.

#### Related Documentation

- [Configuring Flood Defense Settings for Preventing Attacks on page 41](#)
- [Example: Configuring UDP Flooding Protection \(NSM Procedure\) on page 43](#)
- [HTTP Components and MS-Windows Defense Method on page 43](#)

## Configuring Flood Defense Settings for Preventing Attacks

Configure flood defense settings to prevent denial-of-service (DoS) attacks from overwhelming the security device with large numbers or floods of certain packet types. You can protect targets in the security zone from ICMP, SYN, and UDP floods.

- [Configuring ICMP Flooding Protection on page 41](#)
- [Configuring SYN Flooding Protection on page 41](#)
- [Configuring UDP Flooding Protection on page 42](#)

### Configuring ICMP Flooding Protection

An ICMP flood occurs when incoming ICMP echo requests overload a target system with so many requests that the system expends all its resources responding until it can no longer process valid network traffic. You can protect targets in the security zone from ICMP floods by setting a packet-per-second threshold for ICMP requests (default setting: 1000 packets per second). When the ICMP packet flow exceeds the defined threshold, the security device ignores further ICMP echo requests for the remainder of that second and the next second.

### Configuring SYN Flooding Protection

A SYN flood occurs when a target becomes so overwhelmed by SYN segments initiating invalid connection requests that it can no longer process legitimate connection requests. You can configure thresholds for the zone that, when exceeded, prompt the security device to begin acknowledging incoming SYN segments and queuing incomplete

connection requests. Incomplete connection requests remain in the queue until the connection completes or the request times out.

To protect targets in the security zone from SYN floods, enable SYN Flood Protection and configure the thresholds for SYN segments passing through the zone as described in [Table 15 on page 42](#).

**Table 15: Thresholds for SYN segments**

Threshold Types	Your Action
Threshold	Configure the number of SYN packets (TCP segments with the SYN flag set) per second required for the security device to begin SYN proxy. This threshold is the total number of packets passing through the zone, from all sources to all destinations.
Alarm Threshold	Configure the number of proxied TCP connection requests required to generate an alarm in an alarm log entry for the event.
Source Threshold	Configure the number of SYN packets per second from a single IP address required for the security device to begin rejecting new connection requests from that source.
Destination Threshold	Configure the number of SYN packets per second to a single IP address required for the security device to begin rejecting new connection requests to that destination.
Timeout Value	Configure the number of seconds the security device holds an incomplete TCP connection attempt in the proxied connection queue.
Queue Size	Configure the number of proxied TCP connection requests held in the proxied connection queue before the security device begins rejecting new connection requests.

## Configuring UDP Flooding Protection

Security devices currently support UDP for incoming SIP calls. To protect targets in the security zone against UDP flooding by incoming SIP traffic, enable UDP Flooding Protection. The security device can limit the number of UDP packets that can be received by an IP address, preventing incoming SIP calls from overwhelming a target.



**NOTE:** UDP Flood Protection appears only for devices running ScreenOS 5.1 and later.

SIP signaling traffic consists of request and response messages between client and server and uses transport protocols such as UDP or TCP. The media stream carries the data (for example, audio data), and uses Application Layer protocols such as RTP (Real-Time Transport Protocol) over UDP.

### Related Documentation

- [Predefined Screen Options Overview on page 40](#)
- [HTTP Components and MS-Windows Defense Method on page 43](#)
- [Protection Against Scans, Spoofs, and Sweeps on page 44](#)

## Example: Configuring UDP Flooding Protection (NSM Procedure)

In this example, enable UDP Flooding Protection and set a threshold of 80,000 per second for the number of UDP packets that can be received on IP address 1.1.1.5 in the Untrust zone. When this limit is reached, the device generates an alarm and drops subsequent packets for the remainder of that second.

1. Add a NetScreen-208 security device. Choose **Model** when adding the device and configure the device as running ScreenOS 5.1 or later.
2. In the device navigation tree, select **Network > Zone**. Double-click the Untrust zone. The General Properties screen appears.
3. In the zone navigation tree, select **Screen > Flood Defense**, and then click the **UDP Flood Defense** tab.
4. Select **UDP Flood Protection** and ensure that the threshold is set to 1000.
5. Click **OK**.
6. Click the **Add** icon to display the New Destination IP based UDP Flood Protection dialog box. Configure the following options, and then click **OK**:
  - For Destination IP, enter **1.1.1.5**.
  - For Threshold, enter **80000**.
  - Click **OK** to save your changes to the zone, and then click **OK** again to save your changes to the device.

### Related Documentation

- [Configuring Flood Defense Settings for Preventing Attacks on page 41](#)
- [Predefined Screen Options Overview on page 40](#)
- [Interface Types in ScreenOS Devices Overview on page 50](#)

## HTTP Components and MS-Windows Defense Method

Attackers might use HTTP to send ActiveX controls, Java applets, .zip files, or .exe files to a target system, enabling them to load and control applications on hosts in a protected network. You can configure the security device to block the components (the device monitors incoming HTTP headers for blocked content types) as described in [Table 16 on page 43](#).

Table 16: HTTP Components

HTTP Components	Description
Java	Java applets enable Web pages to interact with other programs. The applet runs by downloading itself to the Java Virtual Machine (VM) on a target system. Because attackers can program Java applets to operate outside the VM you might want to block them from passing through the security device.

Table 16: HTTP Components (*continued*)

HTTP Components	Description
ActiveX	Microsoft's ActiveX enables different programs to interact with each other and might contain Java applets, .exe files, or .zip files. Web designers use ActiveX to create dynamic and interactive Web pages that function similarly across different operating systems and platforms. However, attackers might use ActiveX to gain control over a target computer system. When blocking ActiveX components, the security device also blocks Java applets, .exe files, and .zip files whether they are contained within an ActiveX control or not.
ZIP files	Files with .zip extensions contain one or more compressed files, some of which might be .exe files or other potentially malicious files. You can configure the security device to block all .zip files from passing through the zone.
EXE files	Files with .exe extensions might contain malicious code. You can configure the security device to block all .exe files from passing through the zone.

### MS-Windows Defense

Microsoft Windows contains the WinNuke vulnerability, which can be exploited using a DoS attack targeting any computer on the Internet running Microsoft Windows. Attackers can send a TCP segment (usually to NetBIOS port 139 with the urgent (URG) flag set to a host with an established connection; this packet causes a NetBIOS fragment overlap that can crash Windows systems.

To protect targets in the security zone from WinNuke attacks, configure the security device to scan incoming Microsoft NetBIOS session service (port 139) packets for set URG flags. If such a packet is detected, the security device unsets the URG flag, clears the URG pointer, forwards the modified packet, and generates a log entry for the event.

- Related Documentation**
- [Protection Against Scans, Spoofs, and Sweeps on page 44](#)
  - [IP and TCP/IP Anomaly Detection on page 45](#)
  - [Prevention of Security Zones Using Denial of Service Attacks on page 47](#)

## Protection Against Scans, Spoofs, and Sweeps

Attackers often perform address sweeps and/or port scans to gain targeted information about a network. After they have identified trusted addresses or ports, they might launch an attack against the network by spoofing a trusted IP address. To protect targets in the zone from sweeps, scans, and spoofing attempts, configure the detection and blocking settings as described in [Table 17 on page 45](#).



Table 17: Detection and Blocking Settings

Detection and Blocking Settings	Description
IP Address Spoof Protection	<p>Attackers can insert a bogus source address in a packet header to make the packet appear to come from a trusted source. When the interfaces in the zone operate in Route or NAT mode, the security device relies on route table entries to identify IP spoofing attempts. When the interfaces in the zone operate in Transparent mode, the security device relies on address book entries to identify IP spoofing attempts.</p> <ul style="list-style-type: none"> <li>To enable interface-based IP spoofing protection, configure the security device to drop packets that have source IP addresses that do not appear in the route table.</li> <li>To enable zone-based IP spoofing protection (supported on devices running ScreenOS 5.2), configure the security device to drop packets whose source IP addresses do not appear in the selected zone. If you are routing traffic between two interfaces in the same zone, you should leave this option disabled (unchecked).</li> </ul>
IP Address Sweep Protection	<p>An address sweep occurs when one source IP address sends 10 ICMP packets to different hosts within a defined interval. If a host responds with an echo request, attackers have successfully discovered a target IP address. You can configure the security device to monitor ICMP packets from one remote source to multiple addresses. For example, if a remote host sends ICMP traffic to 10 addresses in 0.005 seconds (5000 microseconds), the security device rejects the 11th and all further ICMP packets from that host for the remainder of that second.</p>
Port Scan Protection	<p>A port scan occurs when one source IP address sends IP packets containing TCP SYN segments to 10 different ports at the same destination IP address within a defined interval (5000 microseconds is the default). If a port responds with an available service, attackers have discovered a service to target. You can configure the security device to monitor TCP SYN segments from one remote source to multiple addresses. For example, if a remote host scans 10 ports in 0.005 seconds (5000 microseconds), the security device rejects all further packets from the remote source for the remainder of that second.</p>

**Related Documentation**

- [Configuring Flood Defense Settings for Preventing Attacks on page 41](#)
- [IP and TCP/IP Anomaly Detection on page 45](#)
- [Prevention of Security Zones Using Denial of Service Attacks on page 47](#)

## IP and TCP/IP Anomaly Detection

The Internet Protocol standard RFC 791, *Internet Protocol* specifies a set of eight options that provide special routing controls, diagnostic tools, and security. Attackers can misconfigure IP options to evade detection mechanisms and/or perform reconnaissance on a network.

To detect (and block) anomalous IP fragments as they pass through the zone, configure the settings as described in [Table 18 on page 46](#).

Table 18: IP Setting Options

IP Setting Options	Your Action
Block Bad IP Options	Select this option to block packets with an IP datagram header that contains an incomplete or malformed list of IP options.
Timestamp IP Option Detection	Select this option to block packets in which the IP option list includes option 4 (Internet Timestamp). The timestamp option records the time when each network device receives the packet during its trip from the point of origin to its destination, as well as the IP address of each network device and the transmission duration of each one. If the destination host has been compromised, attackers can discover the network topology and addressing scheme through which the packet passed.
Security IP Option Detection	Select this option for hosts to send security, compartmentation, TCC (closed user group) parameters, and Handling Restriction Codes compatible with U.S. Department of Defense requirements.
Stream IP Option Detection	Select this option to block packets in which the IP option is 8 (Stream ID). Packets must use the 16-bit SATNET stream identifier to be carried through networks that do not support the stream concept.
Record Route IP Option Detection	Select this option to block packets in which the IP option is 7 (Record Route). Attackers might use this option to record the series of Internet addresses through which a packet passes, enabling them to discover network addressing schemes and topologies.
Loose Source IP Option Detection	Select this option to block packets in which the IP option is 3 (Loose Source Routing). The Loose Source Routing option enables the packet to supply routing information used by the gateways when forwarding the packet to the destination; the gateway or host IP can use any number of routes from other intermediate gateways to reach the next address in the route.
Strict Source IP Option Detection	Select this option to block packets in which the IP option is 9 (Strict Source Routing). The Strict Source Routing enables the packet to supply routing information used by the gateways when forwarding the packet to the destination; the gateway or host IP must send the datagram directly to the next address in the source route, and only through the directly connected network indicated in the next address to reach the next gateway or host specified in the route.
Source Route IP Option Filter	Select this option to block all IP traffic that contains the Source Route option. The Source Route option enables the IP header to contain routing information that specifies a different source than the header source. Attackers can use the Source Route option to send a packet with a phony source IP address; all responses to the packet are sent to the attacker's real IP address.

Attackers can craft malicious packets (and packet fragments) that contain anomalies designed to bypass detection mechanisms and gain targeted information about a network. Because different operating systems (OS) respond differently to anomalous packets, attackers can determine the OS running on a target by examining the target's response to the packet. To protect targets in the security zone from these reconnaissance attempts, you can configure the settings as described in [Table 19 on page 47](#).

Table 19: TCP/IP Setting Options

TCP Setting Options	Your Action
SYN Fragment Detection	Select this option to detect TCP fragments that contain a SYN flag. A SYN flag in TCP segment initiates a connection but does not usually contain a payload. Because the packet is small, it should not be fragmented.
Drop Packet without TCP Flags Set	Select this option to detect TCP segment headers that do not have at least one flag control set.
Block SYN with FIN TCP Segments	Select this option to detect packets in which both the SYN and FIN flags are set. The SYN flag synchronizes sequence numbers to initiate a TCP connection and the FIN flag indicates the end of data transmission to finish a TCP connection, so both flags should never be set in the same packet.
Block FIN without ACK TCP Segments	Select this option to detect packets in which the FIN flag is set, but the ACK flag is not. The FIN flag signals the conclusion of a session and terminates the connection; normally the ACK flag is also set to acknowledge the previous packet received.
Drop Packets with an Unknown Protocol	Select this option to drop packets in which the protocol field is set to 101 or greater. Protocol types 101 and higher are currently reserved and undefined.

**Related Documentation**

- [Prevention of Security Zones Using Denial of Service Attacks on page 47](#)
- [Malicious URL Protection on page 49](#)
- [Example: Enabling the Malicious URL Blocking Option \(NSM Procedure\) on page 50](#)

## Prevention of Security Zones Using Denial of Service Attacks

Attackers use denial-of-service (DoS) attacks to overwhelm a target with traffic from a single source IP, preventing the target from processing legitimate traffic. A more advanced version of a DoS attack is a distributed DoS (DDoS) attack, in which attackers use multiple source addresses. Typically, attackers use a spoofed IP address or a previously compromised IP address as the source address to avoid detection.

To protect targets in the security zone from DoS and DDoS attacks, configure the settings as described in [Table 20 on page 47](#).

Table 20: Security Zones Prevention using DoS

Security Zones Setting Options	Your Action
Ping of Death Attack Protection	Select this option to reject oversized and irregular ICMP packets. Attackers might send a maliciously crafted ping (ICMP packet) that is larger than the allowed size of 65,507 bytes to cause a DoS.

Table 20: Security Zones Prevention using DoS (*continued*)

Security Zones Setting Options	Your Action
Teardrop Attack Protection	Select this option to send teardrop attack packets, designed to exploit vulnerabilities in the reassembly of fragmented IP packets. In the IP header, the fragment offset field indicates the starting position, or "offset," of the data contained in a fragmented packet relative to the data of the original unfragmented packet. When the sum of the offset and size of one fragmented packet differ from that of the next fragmented packet, the packets overlap, and the server attempting to reassemble the packet can crash.
Block ICMP Fragments	Select this option to block ICMP packets with the More Fragments flag set or with an offset value in the offset field. ICMP packets are typically very short messages containing error reports or network probe information. Because ICMP packets do not carry large payloads, they should not be fragmented.
Block Large ICMP Packets	Select this option to block ICMP packets larger than 1024 bytes. ICMP packets are typically very short messages containing error reports or network probe information; a large ICMP packet is suspicious.
Block IP Packet Fragments	Select this option to block IP fragments destined for interfaces in the security zone. As packets traverse different networks, it is sometimes necessary to break a packet into smaller pieces (fragments) based upon the maximum transmission unit (MTU) of each network. Attackers can use IP fragments to exploit vulnerabilities in the packet reassembly code of specific IP stack implementations.
Land Attack Protection	Select this option to block SYN floods and IP spoofing combinations. Attackers can initiate a land attack by sending spoofed SYN packets that contain the IP address of the target as both the destination and source IP address. The target responds by sending the SYN-ACK packet to itself, creating an empty connection that lasts until the idle timeout value is reached; in time, these empty connections overwhelm the system.
SYN-ACK-ACK Proxy Protection	Select this option and configure a threshold to prevent SYN-ACK-ACK sessions from flooding the security device session table. After successfully receiving a login prompt from the security device, attackers can continue initiating SYN-ACK-ACK sessions, flooding the security device session table and causing the device to reject legitimate connection requests. When proxy protection is enabled and the number of connections from the same IP address reaches the SYN-ACK-ACK proxy threshold, the security device rejects further connection requests from that IP address. By default, the threshold is 512 connections from any single IP address; you can customize this threshold (1 to 250,000) to meet your networking requirements.
Source IP-Based Session Limit	Select this option and configure a threshold to limit the number of concurrent sessions from the same source IP address. The default threshold is 128 sessions; you can customize this threshold to meet your networking requirements.
Destination IP-Based Session Limit	Select this option and configure a threshold to limit the number of concurrent sessions to the same destination IP address. The default threshold is 128 sessions; you can customize this threshold to meet your networking requirements.

- Related Documentation**
- [IP and TCP/IP Anomaly Detection on page 45](#)
  - [Protection Against Scans, Spoofs, and Sweeps on page 44](#)
  - [Predefined Screen Options Overview on page 40](#)

## Malicious URL Protection

Enable malicious URL protection on a security device to drop incoming HTTP packets that reference URLs with specific user-defined patterns. You can define up to 48 malicious URL string patterns per zone, each of which can be up to 64 characters long, for malicious URL protection at the zone level. When the malicious URL blocking feature is selected, the security device examines the data payload of all HTTP packets. If it locates a URL and detects that the beginning of its string—up to a specified number of characters—matches the pattern you defined, the device blocks that packet from passing the firewall.

A resourceful attacker, realizing that the string is known and might be guarded against, can deliberately fragment the IP packets or TCP segments to make the pattern unrecognizable during a packet-by-packet inspection. However, security devices use Fragment Reassembly to buffer fragments in a queue, reassemble them into a complete packet, and then inspect that packet for a malicious URL. Depending on the results of this reassembly process and subsequent inspection, the device performs one of the following steps:

- If the device discovers a malicious URL, it drops the packet and enters the event in the log.
- If the device cannot complete the reassembly process, a time limit is imposed to age out and discard fragments.
- If the device determines that the URL is not malicious but the reassembled packet is too big to forward, the device fragments that packet into multiple packets and forwards them.
- If the device determines that the URL is not malicious and does not need to fragment it, it then forwards the packet.

To configure a malicious URL string, you must specify the following properties:

- Malicious URL ID—Enter the ID that you want to use to identify the URL string.
- HTTP Header Pattern—Enter the malicious URL string (also called a pattern) that you want the security device to match.
- Minimum Length Before CRLF—Enter the number of characters in the URL string (pattern) that must be present in a URL—starting from the first character—for a positive match (not every character is required for a match). CRLF represents “carriage return/line feed” ; HTTP uses a CR or LF character to mark the end of a code segment.

For more information about malicious URLs on security devices, refer to the *Concepts & Examples ScreenOS Reference Guide: Attack Detection and Defense Mechanisms*.

### Related Documentation

- [Example: Enabling the Malicious URL Blocking Option \(NSM Procedure\) on page 50](#)
- [Predefined Screen Options Overview on page 40](#)
- [Interface Types in ScreenOS Devices Overview on page 50](#)

## Example: Enabling the Malicious URL Blocking Option (NSM Procedure)

---

In this example, you define three malicious URL strings and enable the malicious URL blocking option. Then, enable fragment reassembly for the detection of the URLs in fragmented HTTP traffic arriving at an Untrust zone interface.

1. Add a NetScreen-5GT security device. Choose **Model** when adding the device and configure the device as running ScreenOS 5.x.
2. In the device navigation tree, select **Network > Zone**. Double-click the Untrust zone. The General Properties screen appears.
3. Select **TCP/IP Reassembly for ALG**.
4. In the Zone navigation tree, select **Mal-URL**. Configure three malicious URL strings:
  - a. Click the **Add** icon to display the new Malicious URL ID dialog box. Configure the following and click **OK**:
    - For Malicious URL ID, enter **Perl**.
    - For HTTP Header Pattern, enter **scripts/perl.exe**.
    - For Minimum Length Before CRLF, enter **14**.
  - b. Click the **Add** icon to display the new Malicious URL ID dialog box. Configure the following options, and then click **OK**:
    - For Malicious URL ID, enter **CMF**.
    - For HTTP Header Pattern, enter **cgi-bin/phf**.
    - For Minimum Length Before CRLF, enter **11**.
  - c. Click the **Add** icon to display the new Malicious URL ID dialog box. Configure the following options, and then click **OK**:
    - For Malicious URL ID, enter **DLL**.
    - For HTTP Header Pattern, enter **210.1.1.5/msadcs.dll**.
    - For Minimum Length Before CRLF, enter **18**.
    - Click **OK** to save your changes to the zone, and then click **OK** again to save the device configuration.

- Related Documentation**
- [Predefined Screen Options Overview on page 40](#)
  - [Malicious URL Protection on page 49](#)

## Interface Types in ScreenOS Devices Overview

---

The Interface screen displays the physical interfaces available on the security device. Some security devices support *functional zone interfaces*, which are either a separate

physical MGMT interface for management traffic or a high availability (HA) interface used to link two devices together to form a redundant group or cluster.

Interfaces and subinterfaces enable traffic to enter and exit a security zone. To enable network traffic to flow in and out of a security zone, you must bind an interface to that zone and, if it is a Layer 3 zone, assign it an IP address. You can assign multiple interfaces to a zone, but you cannot assign a single interface to multiple zones.



**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 this information by going to the Juniper website (<http://www.juniper.net/>).

### Interface Types

You can add the interfaces on a security device as described in [Table 21 on page 51](#).

**Table 21: Interface Types**

Interface Types	Description
Aggregate interface	A logical interface that combines two or more physical interfaces on the device, for the purpose of sharing the traffic load to a single IP address. This type of interface is only supported on certain security device systems.
Multilink interface	On available devices, you configure and access multiple serial links called a bundle, through a virtual interface called a multilink interface. The multilink interface emulates a physical interface for the transport of frames.
Loopback interface	A logical interface that emulates a physical interface and is always in the up state.
Virtual security interfaces (VSIs)	The virtual interfaces that two security devices share when forming a virtual security device (VSD) in a high availability cluster.
Redundant interface	Two physical interfaces bound to the same security zone. One of the two physical interfaces acts as the primary interface and handles all the traffic directed to the redundant interface; the other physical interface acts as a backup.
Subinterface	A logical division of a physical interface. A subinterface borrows the bandwidth it needs from the physical interface.
Tunnel interface	Acts as a doorway to a VPN tunnel. Traffic enters and exits a VPN tunnel through a tunnel interface. When you configure a tunnel interface, you can also encapsulate IP multicast packets in GREv1 unicast packets.
ADSL interface	A NetScreen-5GT ADSL security device uses ATM as its Transport Layer. The interface can support multiple permanent virtual circuits (PVCs) on a single physical line. Before you can configure the adsl1 interface, however, you must obtain the DSLAM configuration details for the ADSL connection from the service provider.

Table 21: Interface Types (*continued*)

Interface Types	Description
WAN subinterface	A logical division of a physical WAN interface. This type of interface is only supported on available devices.
ISDN BRI interface	Integrated Services Digital Network (ISDN) is an international communications standard for sending voice, video, and data over digital telephone lines. ISDN in NSM supports Basic Rate Interface (BRI).
Wireless interface	A NetScreen-5GT Wireless security device interface handles wireless traffic to and from that wireless access point (WAP).

For information about configuring specific interface types, see [“Example: Configuring an Aggregate Interface \(NSM Procedure\)” on page 77](#).

**Related Documentation**

- [Configuring Physical and Function Zone Interfaces in ScreenOS Devices Overview on page 52](#)
- [Setting Interface Properties Using the General Properties Screen on page 53](#)
- [Setting Physical Link Attributes for Interfaces on page 55](#)

## Configuring Physical and Function Zone Interfaces in ScreenOS Devices Overview

In the Interface screens, you can configure the physical interfaces and, if available, the function zone interfaces. Double-click the interface in the Interface screen. For physical and function zone interfaces, you can configure the following settings:

- Interface General Properties
- WAN Properties
- Port Properties
- Interface Advanced Properties
- Interface Service Options
- Dynamic Host Configuration Protocol
- Interface Protocol
  - For information about configuring dynamic routing protocols (BGP, RIP, OSPF, OSPFv3) in the virtual router and on the interfaces, see [“OSPF Protocol Configuration Overview” on page 311](#).
  - For information about configuring multicast routing protocols (PIM-SIM, IGMP, IGMP-Proxy) and multicast route entries, see [“Multicast Route Overview” on page 335](#).
- Interface Secondary IP
- Interface Monitoring



- Generic Routing Encapsulation
- Interface Network Address Translation

For more information about interfaces on security devices, see the “Fundamentals” volume in the *Concepts & Examples ScreenOS Reference Guide*.

**Related Documentation**

- [Interface Types in ScreenOS Devices Overview on page 50](#)
- [Setting Physical Link Attributes for Interfaces on page 55](#)
- [Setting Interface Properties Using the General Properties Screen on page 53](#)

## Setting Interface Properties Using the General Properties Screen

Use the General Properties screen to configure the following properties on an interface:

- Name of the interface.
- Subinterface type.
- Zone to which the interface is bound
- VLAN tag
- Bundle into—Configures virtual interfaces on a Multilink Frame Relay (MLFR) for a user-to-network interface (UNI) on available devices.
- Encapsulation Type—Configures the following encapsulation protocols on WAN interfaces: Frame Relay, Multilink Frame Relay (MLFR), Point-to-Point Protocol (PPP), Multilink PPP (MLPPP), and Cisco High-Level Data Link Control (HDLC) on available devices.
- Loopback interface group to which the interface belongs.
- Redundant interface group to which the interface belongs.
- IP address, netmask, and gateway of the interface.



**NOTE:** NSM does not permit you to unset the management IP address. You can, however, still do this on each separate device out of band, using the CLI, the Web UI, or the supplemental CLI. See “[Configuring Features Unsupported in NSM Using Supplemental CLI Options Overview](#)” on [page 129](#).

- Mode of the interface (NAT or route)
- Full support of IPv6 features for VLAN and loopback interfaces on ISG Series devices. See the *Concepts & Examples ScreenOS Reference Guide: IPv6 Configuration*.
- DNS proxy (for details, see “[DNS Server Configuration Using DNS Settings](#)” on [page 103](#)).
- PPP settings.

- Deny routing to this interface.
- Routing to ACVPN-dynamic.

On ADSL interfaces, you can configure ADSL options such as VPI and VCI, multiplexing mode as part of the General Properties. See [“ADSL Interface in ScreenOS Devices” on page 88](#).

On wireless interfaces, you also shut down the interface by selecting the **Shutdown Interface** option.

Some interfaces, such as the VLAN1 or serial interface, accept service option settings as part of the General Properties for the interface. For information about service options, see [“Enabling Management Service Options for Interfaces” on page 56](#).

- Related Documentation**
- [Configuring Physical and Function Zone Interfaces in ScreenOS Devices Overview on page 52](#)
  - [Setting Physical Link Attributes for Interfaces on page 55](#)

---

## Setting WAN Properties Using the WAN Properties Screen

Use the WAN Properties screen to configure the following WAN properties for port cards on available devices:

- Clocking
- Hold time (Up)
- Hold time (Down)

For more information about configuring WAN properties for port cards, refer to the *ScreenOS Wide Area Network Interfaces and Protocols Reference*.

- Related Documentation**
- [Setting Interface Properties Using the General Properties Screen on page 53](#)
  - [Setting Port Properties Using the Port Properties Screen on page 54](#)
  - [Using MLFR and MLPPP Options on page 55](#)

---

## Setting Port Properties Using the Port Properties Screen

Use the Port Properties screen to configure the following properties for port cards on available devices:

- Port Configuration (Serial, E1, T1, or DS3)
- DCE options
- DTE options
- Line encoding

- Loopback mode
- Encapsulation support

For more information about configuring properties, refer to the *ScreenOS Wide Area Network Interfaces and Protocols Reference*.

**Related  
Documentation**

- [Using MLFR and MLPPP Options on page 55](#)
- [Setting Interface Properties Using the General Properties Screen on page 53](#)
- [Setting Physical Link Attributes for Interfaces on page 55](#)

---

## Using MLFR and MLPPP Options

Use the MLFR and MLPPP screens to change the default Frame Relay and PPP properties on a multilink interface. For more information about configuring Frame Relay properties, refer to the *ScreenOS Wide Area Network Interfaces and Protocols Reference*.

**Related  
Documentation**

- [Setting Port Properties Using the Port Properties Screen on page 54](#)
- [Setting Physical Link Attributes for Interfaces on page 55](#)

---

## Setting Physical Link Attributes for Interfaces

Set attributes of the physical link for the interface:

- Physical Settings.
  - Extended Bandwidth Settings—Use the Egress Bandwidth options to set the minimum (or guaranteed) and maximum bandwidth allowed to pass through the security device. Be careful not to allocate more bandwidth than the interface can support because you might lose data if the guaranteed bandwidth on contending policies surpasses the traffic bandwidth set on the interface.

For security devices running ScreenOS 5.3, you can also manage the flow of traffic through the security device by limiting bandwidth at the point of ingress. To configure the maximum amount of traffic allowed at the point of ingress interface, set the number of kilobits per second (kbps) using the Ingress Minimum Bandwidth field.

For more information about configuring traffic shaping parameters, see [“Allocating Network Bandwidth Using Traffic Shaping Options” on page 119](#).

- Holddown Time—Use this option to configure the amount of time (in milliseconds) that the security device uses to bring the interface up or down after detecting a change in the link status.
- Bring Down Link—Select this option to bring down the physical link to the interface.
- Link and MTU Size.
- WebAuth

- **Enable Webauth**—Select this option to enable device administrators to authenticate management connections to the device using WebAuth.
- **WebAuth IP**—Enter the IP address of the WebAuth service on the interface.
- **Allow Webauth via SSL only (ScreenOS 5.1 and later only)**—Select this option to require WebAuth users to use SSL when connecting to the WebAuth IP address on a device running ScreenOS 5.1 and later. When this option is disabled, device administrators can access the WebAuth IP address of the interface using clear text.



**NOTE:** When you enable WebAuth, you must also enable SSL as a service option for the interface. For details, see [“Enabling Management Service Options for Interfaces” on page 56](#).

- **Gratuitous ARP**—To avoid G-ARP attacks by allowing users to enable or disable G-ARP on devices running on ScreenOS 6.1 or later.
- **Deny Routing.**
- **Port Settings.**
- **Proxy ARP Entry**—Import ARP traffic to the correct VSI by allowing the administrator to set the proxy ARP entry with lower and upper IP addresses. By adding a proxy ARP entry on an interface, ScreenOS imports the traffic that is destined to the IP range using this interface.

**Related  
Documentation**

- [Interface Network Address Translation Using VIPs on page 65](#)
- [Interface Network Address Translation Using DIPs on page 67](#)

## Enabling Management Service Options for Interfaces

Enable management service options for the interface as described in [Table 22 on page 56](#).

**Table 22: Management Service Options**

Service Options	Your Action
Web	Select this option to enable the interface to receive HTTP traffic for management from the Web UI.
Telnet	Select this option to enable Telnet manageability. A terminal emulation program for TCP/IP networks such as the Internet, Telnet is a common way to remotely control network devices.
SSH	Administer the security device from an Ethernet connection or a dial-in modem using SSH. You must have an SSH client that is compatible SSHv1.5. These clients are available for Windows 95 and later, Windows NT, Linux, and UNIX. The security device communicates with the SSH client through its built-in SSH server, which provides device configuration and management services. Selecting this option enables SSH manageability.

Table 22: Management Service Options (*continued*)

Service Options	Your Action
SNMP	Select this option to enable SNMP manageability. The security device supports both SNMPv1 and SNMPv2c, and all relevant Management Information Base II (MIB II) groups, as defined in RFC1213.
SSL	Select this option to enable the interface to receive HTTPS traffic for secure management of the security device using the Web UI. Additionally, when this option is enabled, you can also require WebAuth users to use SSL when connecting to the WebAuth IP address on a device running ScreenOS 5.1 and later.
Global Pro (Security Manager)	Select this option to enable the interface to receive NSM traffic.
Ping	Select this option to enable the interface to respond to an ICMP echo request, or ping, which determines whether a specific IP address is accessible over the network.
Ident-Reset	Select this option to restore access that has been blocked by an unacknowledged identification request. Services like Mail and FTP send identification requests. If they receive no acknowledgement, they send the request again. While the request is processing, there is no user access. The Ident-reset option sends a TCP reset announcement in response to an IDENT request to port 113.
NSGP	Select this option to enable the interface to handle NSGP traffic. When enabled, you can also select to enforce IPsec authentication for NSGP traffic.

- Related Documentation**
- [Setting Interface Properties Using the General Properties Screen on page 53](#)
  - [Setting Physical Link Attributes for Interfaces on page 55](#)

## Setting DHCPv6 Overview

An IPv6 router can only be a DHCPv6 server and an IPv6 host can only be a DHCP client. As a DHCPv6 client, the interface can make the following requests from a DHCPv6 server:

- Delegation of long-lived prefixes across an administrative boundary—The server does not have to know the topology of the targeted local network. For example, an ISP can use DHCPv6 to assign prefixes to downstream networks through downstream DHCP clients. To speed up the client/server interaction, the client can request rapid commit (if enabled). Rapid commit reduces the number of messages from four to two.
- IP addresses of available DNS servers—The interface can also request DNS search-list information. This list contains partial domain names, which assist DNS searches by concatenating entered usernames to the domain names.

As a DHCPv6 server, the interface can provide both of these services to a DHCPv6 client. To speed up prefix delegation, an IPv6 router configured to be a DHCPv6 server can support a rapid commit option. You can also set a server preference option.

In the DHCPv6 screen, you can configure options such as a device-unique identification (DUID), an identity association for prefix delegation identification (IAPD-ID), prefix

features, a server preference, a DHCPv6 server, a DHCPv6 client, and a DHCPv6 relay agent

- Related Documentation**
- [Configuring Custom DHCP Options \(NSM Procedure\) on page 59](#)
  - [Using Interface Protocol on page 61](#)

---

## Example: Assigning TCP/IP Settings for Hosts Using DHCP (NSM Procedure)

---

The Dynamic Host Configuration Protocol (DHCP) automatically assigns TCP/IP settings for the hosts on the network. Different security devices support different DHCP roles:

- DHCP clients receive a dynamically assigned IP address.
- DHCP servers allocate dynamic IP addresses to clients.
- DHCP relay agents receive information from a DHCP server and relay that information to clients.

Some devices can simultaneously act as a DHCP client, server, and relay agent.

To assign TCP/IP settings to hosts using DHCP:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Select a security device and then double-click the device on which you want to define forced timeout. The device configuration appears.
3. In the device navigation tree, select **Network > Interface**.
4. Double-click a trust interface. The General Properties screen appears.
5. Select **DHCP** in the navigation tree, and for the DHCP Mode, select **Server**.
6. Configure the server settings as follows:
  - For DHCP Server Auto Processing, select **Enable DHCP Server**.
  - For DNS #1, #2, and #3, enter **1.1.1.1**.
  - For Domain Name, enter **acme.com**.
  - For Client Gateway, enter **1.1.1.1**.
  - For Lease Time (Minutes), the default is 4320 minutes.
  - For Netmask, the default is 0.
  - For NetInfo Server #1 and Server #2, enter **1.1.1.1**.
  - For POP3, enter **1.1.1.1**.
  - For SMTP, enter **1.1.1.1**.
  - For WINS#1 and WINS#2, enter **1.1.1.1**.
  - Select **Enable Next Server IP**.
  - Click **OK** to apply the settings.

**Related Documentation**

- [Setting Interface Properties Using the General Properties Screen on page 53](#)
- [Interface Types in ScreenOS Devices Overview on page 50](#)
- [Configuring Custom DHCP Options \(NSM Procedure\) on page 59](#)

## Configuring Custom DHCP Options (NSM Procedure)

When configuring a DHCP server, you can also configure custom DHCP options to handle address assignment for voice-over-IP (VoIP) phones.



**NOTE:** Custom DHCP options are not supported on the NetScreen-500, the NetScreen-5200, the NetScreen-5400, the ISG1000 and the ISG2000.

A custom DHCP option contains:

- **Option Name**—A user-defined, unique name that identifies the custom option.
- **Code**—An arbitrary integer that represents the option type. Use the option code to represent the custom option you want to configure. For each DHCP server, you can configure an unlimited number of custom DHCP options; however, the option code for each custom option must be unique, and cannot match the option code for a predefined option (DHCP contains several predefined option codes). [Table 23 on page 59](#) lists the predefined option codes and associated RFC 2132 terms:

**Table 23: DHCP Option Codes**

Netmask	1
Gateway	3
DNS1, DNS2, DNS3	6
Domain Name	15
WINS1, WINS2	44
Lease	51
SMTP	69
POP3	70
News	71
NIS1, NIS2	112
NISTAG	113

In addition to predefined option codes, the codes 0, 255, and 53 cannot be used to create a custom DHCP option. All other integers between 2 and 254 are valid.

- **Data Type**—The type of data required for the option code. Available data types are string, IP address, and integer.
- **Value**—The value of the option code. When the data type is string, the acceptable length is 1-128 characters.

Your network recently added support for VoIP, and you now need to support DHCP for VoIP phones. You edit the existing DHCP server configuration to send the following custom options to IP phones acting as DHCP clients:

- Option code 444, containing string "Server 4"
- Option code 66, containing IP address 1.1.1.1
- Option code 160, containing integer 2004

The example assumes that you have already configured a security device to act as a DHCP server.

To customize your DHCP options:

1. In the NSM navigation tree, select **Device Manager > Devices**. Double-click the device currently handling your DHCP assignments.
2. In the device navigation tree, select **Network > Interface**. Double-click an interface. The General Properties screen appears.
3. In the interface navigation tree, select **DHCP**, set the DHCP mode to **Server**, and then select the **Custom Options** tab.
4. Click the **Add** icon to add the first custom option. Configure the following options, and then click **OK**:
  - For Option Name, enter **IP Address**.
  - For Code, enter **66**.
  - For Data Type, select **IP ADDR**.
  - For Value, enter **1.1.1.1**.
  - Click the **Add** icon to add the second custom option. Configure the options as mentioned in Step 4, and then click **OK**.
5. Click **OK** to save your changes to the interface, and then click **OK** again to save your changes to the device.

**Related Documentation**

- [Example: Assigning TCP/IP Settings for Hosts Using DHCP \(NSM Procedure\) on page 58](#)
- [Enabling Management Service Options for Interfaces on page 56](#)



## Using Interface Protocol

You can enable and configure dynamic routing protocol and multicast protocol operations on the interface:

- For information about dynamic routing protocols (BGP, RIP, OSPF) in the virtual router and on the interfaces, see [“OSPF Protocol Configuration Overview” on page 311](#).
- For information about multicast routing protocols (PIM-SIM, IGMP, IGMP-Proxy) and multicast route entries, see [“Multicast Route Overview” on page 335](#).
- You can also configure RIPng protocol to the interface protocol list. For more information, see the *Concepts & Examples ScreenOS Reference Guide*.

### Related Documentation

- [Using Interface Secondary IP on page 61](#)
- [Enabling ScreenOS Devices for Interface Monitoring on page 61](#)
- [Setting Interface Properties Using the General Properties Screen on page 53](#)

## Using Interface Secondary IP

This option is not available for interfaces in the Untrust zone. Each interface has a single, unique primary IP address. You can also set one or more secondary IP addresses for the interface.

### Related Documentation

- [Setting Interface Properties Using the General Properties Screen on page 53](#)
- [Example: Assigning TCP/IP Settings for Hosts Using DHCP \(NSM Procedure\) on page 58](#)
- [Using Interface Protocol on page 61](#)

## Enabling ScreenOS Devices for Interface Monitoring

You can enable the security device to monitor the reachability of certain IP addresses through the interface to determine interface failure. For each IP address to be tracked, specify the following:

- Interval at which pings are sent to the tracked address
- Number of consecutive unsuccessful ping attempts before the connection to the address is considered failed
- Weight of the failed IP connection
- Timeout for the track IP

The Failover Threshold is compared to the sum of the weights of failed IP connections. Instead of tracking specific IP addresses, you can alternatively set the device to track the interface's default gateway.

- Related Documentation**
- [Using Interface Protocol on page 61](#)
  - [Using Interface Secondary IP on page 61](#)
  - [Setting Interface Properties Using the General Properties Screen on page 53](#)

---

## Supporting Generic Routing Encapsulation Using Tunnel Interfaces

You can configure a tunnel interface to support Generic Routing Encapsulation version 1 (GREv1) encapsulation. When enabled, the interface encapsulates IP packets in the tunnel in IPv4 packets using GREv1. You must specify the key parameter to append the value to outgoing packets (incoming packets must have this value too).

You can use GRE to forward multicast packets through non-multicast aware routers and devices.

- Related Documentation**
- [Setting Interface Properties Using the General Properties Screen on page 53](#)
  - [Configuring Physical and Function Zone Interfaces in ScreenOS Devices Overview on page 52](#)

---

## Interface Network Address Translation Methods

You can configure the following address translation methods on the security device:

- MIPs
- VIPs
- Mapping services and ports
- DIPs
- Port Address Translation
- DIP with extended Interface
- Incoming DIP for SIP traffic

- Related Documentation**
- [Interface Network Address Translation Using MIPs on page 62](#)
  - [Interface Network Address Translation Using VIPs on page 65](#)
  - [Interface Network Address Translation Using DIPs on page 67](#)

---

## Interface Network Address Translation Using MIPs

A mapped IP (MIP) is a direct one-to-one mapping of one IP address to another. The security device forwards incoming traffic destined for a MIP to the host with the address to which the MIP points. A MIP is a static destination address translation that maps the destination IP address in an IP packet header to another static IP address, enabling inbound traffic to reach private addresses in a zone whose interface is in NAT mode. When a MIP host initiates outbound traffic, the security device translates the source IP

address of the host to that of the MIP address. You can map an address-to-address or subnet-to-subnet relationship (the netmask applies to both the mapped IP subnet and the original IP subnet).

You can also use a MIP to handle overlapping address spaces at two sites connected by a VPN tunnel (an overlapping address space is when the IP address range in two networks are partially or completely the same).

However, devices running ScreenOS 6.1 or later remove the overlap restriction between the MIP and the VIP.

The zone you configure the MIP in determines the subnet of IP address that you can assign the MIP:

- When defining a MIP in a tunnel zone or security zone other than untrust, you must use the same subnet as a tunnel interface with an IP address and netmask, or in the same subnet as the IP address and netmask of an interface bound to a Layer 3 (L3) security zone.
- When defining a MIP in an interface in the Untrust zone, you can use a different subnet than the Untrust zone interface IP address. However, you must add a route on the external router pointing to an Untrust zone interface so that incoming traffic can reach the MIP. You must also define a static route that associates the MIP with the interface that hosts it.
- With devices running ScreenOS 6.1 or later, you can assign a MIP the same address as an interface on any platform. However, you cannot use that MIP address in a DIP pool.

You can use a MIP as the destination addresses in rules between any two zones or in a Global rule. For the destination zone, use either the Global zone or the zone with the address to which the MIP points.

#### Related Documentation

- [Interface Network Address Translation Methods on page 62](#)
- [Example: Configuring MIPs \(NSM Procedure\) on page 63](#)
- [Interface Network Address Translation Using VIPs on page 65](#)

### Example: Configuring MIPs (NSM Procedure)

In this example, you create a MIP to handle inbound traffic to your Web server. After configuring the MIP, you create a Global MIP to represent the MIP you created for the device, and then use the Global MIP object in a Security Policy rule that permits HTTP traffic from any address in the Untrust zone to the MIP—and to the host with the address to which the MIP points—in the Trust zone. All security zones are in the trust-vr routing domain.

To configure a MIP:

1. Add a NetScreen-50 security device. Choose **Model** when adding the device and configure the device as running ScreenOS 5.x.
2. Configure the Trust interface for ethernet1.

- In the device navigation tree, select **Network > Interface**.
  - Double-click **ethernet1** (trust interface). The General Properties screen appears.
  - Configure the IP address as 10.1.1.1 and the Netmask as 24. Leave all other settings as default.
  - Click **OK** to save your changes.
3. Configure the Untrust interface for ethernet2.
    - In the device navigation tree, select **Network > Interface**.
    - Double-click **ethernet2** (untrust interface). The General Properties screen appears.
  4. Configure the IP address as 1.1.1.1 and the netmask as 24. Leave all other settings as default.
    - Click **OK** to save your changes.
  5. In the interface navigation tree, select **NAT > MIP** to display the MIP screen.
  6. Click the **Add** icon and configure the following:
    - For Mapped IP, enter **1.1.1.5**.
    - For Netmask, enter **32**.
    - For Host IP, enter **10.1.1.5**.
    - For virtual router, select **trust-vr**.
    - Click **OK** to save the MIP.
  7. Click **OK** to save your changes to the interface, and then click **OK** to save your changes to the device.
  8. Create a Global MIP to reference the MIP you created for the device. You use a Global MIP when configuring NAT in a Security Policy rule; the Global MIP references the MIP for an individual device, enabling you to use one object (the Global MIP object) to represent multiple MIPs in a single rule.
  9. In the navigation tree, select **Object Manager > NAT Objects > MIP**.
  10. Click the **Add** icon to display the new Global MIP dialog box.
  11. Configure the Global MIP.
  12. Configure a firewall rule to route inbound HTTP traffic to the MIP address.

**Related Documentation**

- [Interface Network Address Translation Using MIPs on page 62](#)
- [Interface Network Address Translation Using DIPs on page 67](#)
- [Interface Network Address Translation Methods on page 62](#)

## Interface Network Address Translation Using VIPs

A virtual IP (VIP) address maps traffic received at one IP address to another address based on the destination port number in the TCP or UDP segment header. The destination IP addresses are the same, and the destination port numbers determine the host that receives the traffic. The security device forwards incoming traffic destined for a VIP to the host with the address to which the VIP points. When a VIP host initiates outbound traffic, the security device translates the source IP address of the host to that of the VIP address.

You can set a VIP only on an interface in the Untrust zone, and you must assign the VIP an IP address that is in the same subnet as an interface in the Untrust zone. However, in devices running ScreenOS 6.1 or later, you can set an interface in a Layer 3 security zone, removing the restriction of setting an Untrust zone interface. Some security devices also support:

- Assigning the VIP the exact same address as the interface. However, in devices running ScreenOS 6.1 or later, you can set a VIP as you would an interface IP in any platform, removing the restriction of some devices.
- Assigning the VIP to a dynamic IP address. When using a VIP with an interface in the Untrust zone that receives its IP address dynamically through DHCP or PPPoE, select **Same as the untrusted interface IP address** when setting up the VIP.

Additionally, the host to which the security device maps VIP traffic must be reachable from the trust-vr. If the host is in a routing domain other than that of the trust-vr, you must define a route to reach it.

You can use a VIP as the destination address in rules between any two zones or in a Global rule. For the destination zone, use either the Global zone or the zone with the address to which the VIP points.

### Related Documentation

- [Mapping Predefined and Custom Services in a VIP on page 65](#)
- [Interface Network Address Translation Methods on page 62](#)

## Mapping Predefined and Custom Services in a VIP

You can use virtual port numbers for well-known services when running multiple server processes on a single machine. For example, you can run two FTP servers on the same machine, one server on port 21 and the other on port 2121. Only users who know the virtual port number can append it to the IP address in the packet header to gain access to the second FTP server.

You can map predefined and custom services in a VIP. A single VIP can support custom services with:

- The same source and destination port numbers but different transports.
- Single port entries (by default).

- Multiple port entries, when creating multiple service entries under a VIP (one service entry in the VIP for each port entry in the service).
- Any destination port number or number range from 1 to 65,535, not just from 1024 to 65,535.

**Related  
Documentation**

- [Interface Network Address Translation Using VIPs on page 65](#)
- [Example: Configuring VIPs \(NSM Procedure\) on page 66](#)
- [Interface Network Address Translation Methods on page 62](#)

---

## Example: Configuring VIPs (NSM Procedure)

In this example, you create a VIP to handle inbound traffic to your Web server. After configuring the VIP, you create a Global VIP to represent the VIP you created for the device, and then use the Global VIP object in a Security Policy rule that permits HTTP traffic on port 80 from any address in the Untrust zone to the MIP—and to the host with the address and port to which the MIP points—in the Trust zone. All security zones are in the trust-vr routing domain.

Because the VIP is in the same subnet as the Untrust zone interface, you do not need to define a route for traffic from the Untrust zone to reach it. (To route HTTP traffic from a security zone other than the Untrust zone to the VIP, you must set a route for 1.1.1.10 on the router in the other zone to point to an interface bound to that zone.)

1. Add a NetScreen-204 security device. Choose **Model** when adding the device and configure the device as running ScreenOS 5.x.
2. Configure the Trust interface for ethernet1.
3. In the device navigation tree, select **Network > Interface**.
4. Double-click **ethernet1** (trust interface). The General Properties screen appears.
5. Configure the IP address as 10.1.1.1 and the netmask as 24. Leave all other settings as default.
6. Click **OK** to save your changes.
7. Configure the Untrust interface for ethernet3.
8. In the device navigation tree, select **Network > Interface**.
9. Double-click **ethernet3** (untrust interface). The General Properties screen appears.
10. Configure the IP address as 1.1.1.1 and the netmask as 24. Leave all other settings as default.
11. Click **OK** to save your changes.
12. Configure the VIP for ethernet3:
  - Double-click **ethernet3**. The General Properties screen appears.
  - In the interface navigation tree, select **NAT > VIP** to display the VIP screen.

- Click the **Add** icon to display the Virtual IP dialog box. Enter the Virtual IP as **1.1.1.10**.
13. Click the **Add** icon to display the VIP mapping dialog box. Configure the following options:
    - For Virtual Port, enter **80**.
    - For Mapped IP, enter **10.1.1.10**.
    - For Mapped Service, enter **HTTP**.
    - Click **OK** to save the VIP mapping, and then click **OK** to save the VIP.
    - Click **OK** to save your changes to the interface, and then click **OK** to save your changes to the device.
  14. In the navigation tree, select **Object Manager > NAT Objects > VIP**.
  15. Click the **Add** icon to display the new Global VIP dialog box.
  16. Configure the Global VIP.
  17. Configure a firewall rule to route inbound HTTP traffic on port 80 to the VIP address.

**Related  
Documentation**

- [Interface Network Address Translation Using VIPs on page 65](#)
- [Interface Network Address Translation Methods on page 62](#)
- [Mapping Predefined and Custom Services in a VIP on page 65](#)

## Interface Network Address Translation Using DIPs

A dynamic IP (DIP) pool is a range of IP addresses. The security device can dynamically or deterministically use these IP addresses when performing network address translation on the source IP address (NAT-src) in IP packet headers.

- If the range of addresses in a DIP pool is in the same subnet as the interface IP address, the pool must exclude the interface IP address, router IP addresses, and any mapped IP (MIP) or virtual IP (VIP) addresses that might also be in that subnet.
- If the range of addresses is in the subnet of an extended interface, the pool must exclude the extended interface IP address.

You can assign DIP pools to physical interfaces and subinterfaces for network and VPN traffic, and tunnel interfaces for VPN tunnels only.

Dip pools can now be defined on VLAN interface when the device running on ScreenOS 6.2 is in Transparent mode.

**Related  
Documentation**

- [Example: Enabling Multiple Hosts Using Port Address Translation \(NSM Procedure\) on page 68](#)
- [Example: Translating Source IP Addresses into a Different Subnet \(NSM Procedure\) on page 69](#)
- [Enabling Managed Devices Using Incoming DIP on page 73](#)

## Example: Enabling Multiple Hosts Using Port Address Translation (NSM Procedure)

Use Port Address Translation (PAT) to enable multiple hosts (up to 64,500) to share the same IP address. The security device maintains a list of assigned port numbers to distinguish which session belongs to which host. Use PAT in conjunction with a MIP and a DIP pool to resolve the problem of overlapping address spaces.

Some applications, such as NetBIOS Extended User Interface (NetBEUI) and Windows Internet Naming Service (WINS), require specific port numbers and do not work with PAT. For these applications, you cannot use PAT; you must configure the DIP pool to use a fixed port (numbered IP). For fixed-port DIP, the security device hashes and saves the original host IP address in its host hash table, enabling the device to associate the right session with each host.

In this example, you want to create a VPN tunnel for users at one site to reach an FTP server at another site. However, the internal networks at both sites use the same private address space of 10.1.1.0/24.

On the first device, an NetScreen-HSC, you create a tunnel interface in the Untrust zone with IP address 10.10.1.1/24, and associate it with a DIP pool containing the IP address range 10.10.1.2–10.10.1.2 (addresses in the neutral address space of 10.10.1.0/24). You enable port address translation for the DIP pool. On the second device, an NetScreen-208, you create a tunnel interface with an IP address in a neutral address space and set up a mapped IP (MIP) address to its FTP server. This example provides details on configuring the NetScreen-HSC to use a DIP pool with PAT; details on configuring the second device in the VPN are not provided.

1. Add a NetScreen-HSC security device. Choose **Model** when adding the device and configure the device as running ScreenOS 5.x and ScreenOS 6.2 in Transparent mode.
2. Configure the tunnel/vlan interface:
  - In the device navigation tree, select **Network > Interface**.
  - Click the **Add** icon and select **New > Tunnel** or **Vlan Interface**. The General Properties screen appears.
3. Configure the DIP pool:
  - In the interface navigation tree, select **NAT > DIP** to display the DIP screen.
  - Click the **Add** icon to display the New Dynamic IP dialog box.
4. Enter the DIP ID.
5. Add multiple DIP ranges for a particular DIP ID as follows:
  - Select the **Multiple DIP Range** check box.
  - Click the **Add** icon. The New Dynamic IP dialog box appears.
  - For Rang ID, enter **1**.



- For Lower IP, enter **10.10.1.2**.
  - For Upper IP, enter **10.10.1.2**.
6. For Start, enter **10.10.1.1**.
  7. For End, enter **10.10.1.1**.
  8. For Netmask, enter **24**.
  9. Click **OK** to save your changes to the interface, and then click **OK** to save your changes to the device.

**Related Documentation**

- [Example: Translating Source IP Addresses into a Different Subnet \(NSM Procedure\) on page 69](#)
- [Enabling Managed Devices Using Incoming DIP on page 73](#)
- [Interface Network Address Translation Using DIPs on page 67](#)

## Example: Translating Source IP Addresses into a Different Subnet (NSM Procedure)

If circumstances require that the source IP address in outbound firewall traffic be translated to an address in a different subnet from that of egress interface, you can use the extended interface option. This option enables you to graft a second IP address and an accompanying DIP pool onto an interface that is in a different subnet. You can then enable NAT on a per-policy basis and specify the DIP pool built on the extended interface for the translation.

In this example, two branch offices have leased lines to a central office. The central office requires them to use only the authorized IP addresses it has assigned them. However, the offices receive different IP addresses from their ISPs for Internet traffic. For communication with the central office, you use the extended interface option to configure the security device in each branch office to translate the source IP address in packets it sends to the central office to the authorized address. [Table 24 on page 69](#) lists the authorized and assigned IP addresses for branch offices A and B.

**Table 24: Sample Branch Office Addresses**

<b>Office A</b>	195.1.1.1/24	211.10.1.1/24
<b>Office B</b>	201.1.1.1/24	211.20.1.1/24

The security devices at both sites have a Trust zone and an Untrust zone. All security zones are in the trust-vr routing domain. You bind ethernet1 to the Trust zone and assign it IP address 10.1.1.1/24. You bind ethernet3 to the Untrust zone and give it the IP address assigned by the ISPs: 195.1.1.1/24 for Office A and 201.1.1.1/24 for Office B. You then create an extended interface with a DIP pool containing the authorized IP address on ethernet3:

- Office A—extended interface IP 211.10.1.10/24; DIP pool 211.10.1.1 – 211.10.1.1; PAT enabled
- Office B—extended interface IP 211.20.1.10/24; DIP pool 211.20.1.1 – 211.20.1.1; PAT enabled

You set the Trust zone interface in NAT mode. It uses the Untrust zone interface IP address as its source address in all outbound traffic except for traffic sent to the central office. You configure a policy to the central office that translates the source address to an address in the DIP pool in the extended interface. (The DIP pool ID number is 5. It contains one IP address, which, with port address translation, can handle sessions for ~64,500 hosts.) The MIP address that the central office uses for inbound traffic is 200.1.1.1, which you enter as "HQ" in the Untrust zone address book on each security device.

Each ISP must set up a route for traffic destined to a site at the end of a leased line to use that leased line. The ISPs route any other traffic they receive from a local security device to the Internet.

1. Add the devices:
  - For Office A, add a NetScreen-208 security device.
  - For Office B, add a NetScreen-204 security device.
2. Configure ethernet1 (Trust Zone) for Office A:
  - Double-click Office A device to open the device configuration. In the device navigation tree, select **Network > Interface**.
  - Double-click **ethernet1**. The General Properties screen appears.
3. Configure IP address/netmask as 10.1.1.1/24 and Interface Mode as NAT.
4. Click **OK** to save your changes.
5. Configure ethernet3 (Untrust Zone) for Office A:
  - In the device navigation tree, select **Network > Interface**.
  - Double-click **ethernet3**. The General Properties screen appears.
  - Configure IP address/netmask as 195.1.1.1/24 and Interface Mode as Route.
6. In the interface navigation tree, select **NAT > DIP**. Click the **Add** icon to display the New Dynamic IP dialog box. Configure the DIP, and then click **OK**:
7. Enter the DIP ID.
8. Add multiple DIP ranges for a particular DIP ID as follows:
  - Select the **Multiple DIP Range** check box.
  - Click the **Add** icon. The New MultiRange of DIP dialog box appears.
  - For Rang ID, enter **1**.
  - For Lower IP, enter **210.10.1.1**.
  - For Upper IP, enter **210.10.1.1**.
9. For Start, enter **210.10.1.1**.
10. For End, enter **210.10.1.1**.
11. For Shift From, enter **10.10.1.2**.

12. For Scale-Size, enter 1.
13. Select the **Fixed Port** check box.



**NOTE:** The Fixed Port is enabled by default while adding multiple DIP range for a DIP ID.

14. For Extended IP, enter **211.10.1.10**.
15. For Netmask, enter **24**.
16. Add the route to the Corporate Office on the trust-vr of Office A:
  - In the device navigation tree, select **Network > Routing**. Double-click **trust-vr router**. The General Properties screen appears.
17. In the trust-vr navigation tree, select **Routing Table**. Click the **Add** icon and configure the new route:
  - Set the IP address/netmask to 0.0.0.0/0.
  - For Next Hop, select **Gateway**, and the gateway options appear.
  - For Interface, select **ethernet3**.
  - For Gateway IP Address, enter **195.1.1.254**.
18. Leave all other defaults, and then click **OK** to save the route.
19. Click **OK** to save your changes to the trust-vr, and then click **OK** to save your changes and close the Office A device configuration.
20. Configure ethernet1 (Trust Zone) for Office B:
  - Double-click Office B device to open the device configuration. In the device navigation tree, select **Network > Interface**.
  - Double-click **ethernet1**. The General Properties screen appears.
21. Configure IP address/netmask as 10.1.1.1/24 and Interface Mode as NAT.
  - Click **OK** to save your changes.
22. Configure ethernet3 (Untrust Zone) for Office B:
  - In the device navigation tree, select **Network > Interface**.
  - Double-click **ethernet3**. The General Properties screen appears.
  - Configure IP address/netmask as 201.1.1.1/24 and Interface Mode as Route.
23. In the interface navigation tree, select **NAT > DIP**. Click the **Add** icon to display the New Dynamic IP dialog box. Configure the DIP, and then click **OK**.
24. Enter the DIP ID.
25. To add multiple DIP ranges for a particular DIP ID:

- Enable the **Multiple DIP Range** check box.
- Click the **Add** icon to display the New MultiRange of DIP dialog box.
- For Rang ID, enter **1**.
- For Lower IP, enter **10.10.1.2**.
- For Upper IP, enter **10.10.1.2**.

26. For Start, enter **210.10.1.1**.

27. For End, enter **210.10.1.1**.

28. For Shift From, enter **10.10.1.2**.

29. For Scale-Size, enter **1**.

30. Enable the **Fixed Port** check box.



**NOTE:** The Fixed Port is enabled by default while adding multiple DIP range for a DIP ID.

31. For Extended IP, enter **211.10.1.10**.

32. For Netmask, enter **24**.

33. Add the route to the Corporate Office on the trust-vr of Office B:

- In the device navigation tree, select **Network > Routing**. Double-click **trust-vr router**. The General Properties screen appears.

34. In the trust-vr navigation tree, select **Routing Table**. Click the **Add** icon and configure the new route:

- Set the IP address/netmask to **0.0.0.0/0**.
- For Next Hop, select **Gateway**, and the gateway options appear.
- For Interface, select **ethernet3**.
- For Gateway IP Address, enter **201.1.1.254**.
- Leave all other defaults, and then click **OK** to save the route.
- Click **OK** to save your changes to the trust-vr, then click **OK** to save your changes and close the Office A device configuration.

35. Add the Address Object that represents HQ:

- In the main navigation tree, select **Object Manager > Address Objects**. Click the **Add** icon and select **Host**. The New Host dialog box appears.

36. Configure the Host as detailed below, and then click **OK**:

- For Name, enter **Central Office HQ**.
- Select **IP**, and then enter the IP Address **200.1.1.1**.

37. Create a Global DIP to reference the DIP pool on each device. You use a Global DIP when configuring NAT in a firewall rule; the Global DIP references the DIP pool for an individual device, enabling you to use one object (the Global DIP object) to represent multiple DIP pools in a single rule.

- In the navigation tree, select **Object Manager > NAT Objects > DIP**.
- Click the **Add** icon to display the new Global DIP dialog box. Configure the Global DIP and then click **OK**:

38. Configure two firewall rules, one which uses the Global DIP object for NAT translation.

#### Related Documentation

- [Example: Enabling Multiple Hosts Using Port Address Translation \(NSM Procedure\) on page 68](#)
- [Interface Network Address Translation Using DIPs on page 67](#)

## Enabling Managed Devices Using Incoming DIP

Use an incoming DIP to enable the managed device to handle incoming Session Initiation Protocol (SIP) calls. SIP is an Internet Engineering Task Force (IETF)-standard protocol for initiating, modifying, and terminating multimedia sessions (such as conferencing, telephony, or multimedia) over the Internet. SIP is used to distribute the session description, to negotiate and modify the parameters of an existing session, and to terminate a multimedia session.



**NOTE:** SIP is a predefined service that uses port 5060 as the destination port. To specify the SIP service in the Service column of a firewall rule, you must select the predefined service group VoIP, which includes the H.323 and SIP service objects.

To use SIP, a caller must register with the registrar before SIP proxies and location servers can identify where the caller wants to be contacted. A caller can register one or more contact locations by sending a REGISTER message to the registrar. The REGISTER message contains the address-of-record URI and one or more contact URIs. When the registrar receives the message, it creates bindings in a location service that associates the address-of-record with the contact addresses.

The security device monitors outgoing REGISTER messages from SIP users, performs NAT on these addresses, and stores the information in an incoming DIP table. When the device receives an INVITE message from the external network, it uses the incoming DIP table to identify which internal host to route the INVITE message to.

To enable the device to perform NAT on incoming SIP calls, you must configure an interface DIP or DIP pool on the egress interface of the device. A single interface DIP is adequate for handling incoming calls in a small office; a DIP pool is recommended for larger networks or an enterprise environment.



**NOTE:** SIP uses UDP as its transport protocol. When using your managed device to handle SIP traffic, you might also want to enable UDP Flood Protection. For details on configuring UDP Flood Protection, see [“Configuring Flood Defense Settings for Preventing Attacks” on page 41](#).

**Related Documentation**

- [Example: Translating Source IP Addresses into a Different Subnet \(NSM Procedure\) on page 69](#)
- [Example: Enabling Multiple Hosts Using Port Address Translation \(NSM Procedure\) on page 68](#)
- [Interface Network Address Translation Using DIPs on page 67](#)

---

## Example: Configuring Interface-Based DIP (NSM Procedure)

---

In this example, you configure an interface-based DIP on the Untrust interface of the security device, and then configure a firewall rule that permits SIP traffic from the Untrust zone to the Trust zone and references the interface DIP. You also configure a rule that permits SIP traffic from the Trust to the Untrust zone using NAT source, which enables hosts in the Trust zone to register with the proxy in the Untrust zone.

1. Add a NetScreen-208 device named Office A. Choose **Model** when adding each device and configure as running ScreenOS 5.1.
2. Configure ethernet1 (Trust Zone) for Office A:
  - Double-click **Office A** device to open the device configuration. In the device navigation tree, select **Network > Interface**.
  - Double-click **ethernet1**. The General Properties screen appears.
  - Configure IP address/netmask as 10.1.1.1/24 and Interface mode as NAT.
  - Click **OK** to save your changes.
3. Configure ethernet3 (Untrust Zone) for Office A:
  - Double-click **ethernet3**. The General Properties screen appears.
  - Configure IP address/netmask as 1.1.1.1/24.
  - In the interface navigation tree, select **NAT > DIP**, and then click the **Interface DIP** tab.
  - Select **Incoming NAT**.
4. Click **OK** to save your changes to the interface, and then click **OK** again to save your changes to the device.
5. Create a Global DIP to reference the Interface DIP on Office A. You use a Global DIP when configuring NAT in a firewall rule; the Global DIP references the Interface DIP for an individual device.
6. In the navigation tree, select **Object Manager > NAT Objects > DIP**.

7. Click the **Add** icon to display the new Global DIP dialog box.
8. Configure the Global DIP.
9. Configure firewall rules:
  - Rule 1 handles outgoing SIP traffic, and uses the outgoing interface to perform NAT.
  - Rule 2 handles incoming SIP traffic, and uses the Interface DIP as the destination to perform NAT.



**NOTE:** SIP is a predefined service that uses port 5060 as the destination port. To specify the SIP service in the Service column of a firewall rule, you must select the predefined service group VoIP, which includes the H.323 and SIP service objects.

#### Related Documentation

- [Enabling Managed Devices Using Incoming DIP on page 73](#)
- [Example: Translating Source IP Addresses into a Different Subnet \(NSM Procedure\) on page 69](#)
- [Interface Network Address Translation Using DIPs on page 67](#)

### Example: Configuring DIP Pools on the Untrust Interface (NSM Procedure)

In this example, you configure a DIP pool on the Untrust interface to perform NAT on incoming SIP calls. After creating the DIP pool and Global DIP object, you configure a firewall rule to permit SIP traffic from the Untrust zone to the Trust zone and reference the DIP pool. You also configure a rule to permit SIP traffic from the Trust to the Untrust zone, which enables hosts in the Trust zone to register with the proxy in the Untrust zone.

1. Add a NetScreen-204 device named Office B. Choose **Model** when adding each device and configure as running ScreenOS 5.1.
2. Configure ethernet1 (Trust Zone) for Office B:
  - Double-click **Office B** device to open the device configuration. In the device navigation tree, select **Network > Interface**.
  - Double-click **ethernet1**. The General Properties screen appears.
  - Configure IP address/netmask as 10.1.1.1/24 and Interface mode as NAT.
  - Click **OK** to save your changes.
3. Configure ethernet3 (Untrust Zone) for Office B:
  - Double-click **ethernet3**. The General Properties screen appears.
  - Configure IP address/netmask as 1.1.1.1/24.
4. In the interface navigation tree, select **NAT > DIP**, and then click the **Add** icon. The new DIP Pool dialog box appears. Configure as detailed below:

5. Enter the DIP ID.
6. Add multiple DIP ranges for a particular DIP ID:
  - Enable the **Multiple DIP Range** check box.
  - Click the **Add** icon to display the New MultiRange of DIP dialog box.
  - Enter the identification range for Rang ID.
  - For Lower IP, enter the same IP address as the subnet interface IP address.
  - For Upper IP, enter the same IP address as the subnet interface IP address.
7. For Start, enter **1.1.1.20**.
8. For End, enter **1.1.1.40**.
9. For Shift From, enter **1.1.1.20**.
10. For Scale-Size, enter **1**.
11. Select the **Fixed Port** check box.



**NOTE:** The Fixed Port is enabled by default while adding multiple DIP range for a DIP ID.

12. For Extended IP, enter **211.10.1.10**.
13. For Netmask, enter **24**.
14. Select **Incoming NAT**.
15. Click **OK**.
16. Create a Global DIP to reference the Incoming NAT DIP on Office B. You use a Global DIP when configuring NAT in a firewall rule; the Global DIP references the Incoming NAT DIP for an individual device.
  - In the navigation tree, select **Object Manager > NAT Objects > DIP**.
  - Click the **Add** icon to display the new Global DIP dialog box.
17. Configure the Global DIP.
18. Configure firewall rules:
  - Rule 1 handles outgoing SIP traffic and uses the outgoing interface to perform NAT.
  - Rule 2 handles incoming SIP traffic and uses the interface DIP to perform NAT.

**Related  
Documentation**

- [Example: Configuring Interface-Based DIP \(NSM Procedure\) on page 74](#)
- [Interface Network Address Translation Using DIPs on page 67](#)



## Example: Configuring an Aggregate Interface (NSM Procedure)

An aggregate interface combines two or more physical interfaces, enabling each member to share equally the traffic load on the aggregate interface IP address. Use an aggregate interface to increase the amount of bandwidth available to a single IP address. You can also provide redundancy: If one member of an aggregate interface fails, the other members can continue processing traffic—although with less bandwidth than previously available.

The NetScreen-5000 line supports aggregate interfaces with Secure Port Modules (SPMs):

- The 5000-8G SPM supports up to four aggregate interfaces.
- The 5000-24FE SPM supports up to five aggregate interfaces.

You must assign one of the following names to the aggregate interface: aggregate1, aggregate2, aggregate3, aggregate4, or aggregate5.

In this example, you combine two Gigabit Ethernet mini-GBIC ports, each running at 1 Gbps, into an aggregate interface (aggregate1) running at 2Gbps. The aggregate interface combines Ethernet ports 1 and 2 on a NetScreen 5000-8G SPM (residing in Slot 2) and is bound to the Trust zone.

1. Add a NetScreen-5200 device running ScreenOS 5.x, and then configure the network module:
  - Double-click the device icon to open the device configuration. In the device navigation tree, select **Network > Slot**.
  - Double-click slot 2 to display the slot configuration dialog box. For Card Type, select **5000-8G SPM**.
  - Click **OK** to save the slot configuration.
2. Configure the aggregate interface:
  - In the device navigation tree, select **Network > Interface**.
  - Click the **Add** icon and select **Aggregate Interface**. The General Properties screen appears.
3. Configure the following options:
  - For Zone, select **Trust**.
  - For IP address/netmask, enter **10.1.1.0/24**.
  - For Interface Mode, ensure that the mode is set to **NAT**.
  - Click **OK** to save your changes.
4. Add the ethernet 2/1 interface as a member of the aggregate1 interface.
  - In the device navigation tree, select **Network > Interface**. Double-click **ethernet2/1**. The General Properties screen appears.

- Configure the Parent Aggregate Interface as aggregate1.
  - Click **OK** to save your changes.
5. Add the ethernet 2/2 interface as a member of the aggregate1 interface.
    - In the device navigation tree, select **Network > Interface**. Double-click **ethernet2/2**. The General Properties screen appears.
  6. Configure the Parent Aggregate Interface as aggregate1.
  7. Click **OK** to save your changes.

**Related  
Documentation**

- [Example: Configuring a Multilink Interface \(NSM Procedure\) on page 78](#)
- [Interface Types in ScreenOS Devices Overview on page 50](#)

---

## Example: Configuring a Multilink Interface (NSM Procedure)

On available devices, you can configure and access multiple serial links called a bundle, through a virtual interface called a multilink interface. The multilink interface emulates a physical interface for the transport of frames.

In this example, you combine two WAN subinterfaces into an multilink interface. The name of the multilink interface must be *mlid\_num*. For example, multilink interface names can be ml1, ml2, and so on.

1. Add an SSG520 device running ScreenOS 5.1, and then configure the network module:
  - Double-click the device icon to open the device configuration. In the device navigation tree, select **Network > Slot**.
  - Double-click **slot 2** to display the slot configuration dialog box. Select a card type.
  - Click **OK** to save the slot configuration.
2. Configure the multilink interface:
  - In the device navigation tree, select **Network > Interface**.
  - Click the **Add** icon and select **Multilink Interface**. The General Properties screen appears.
3. Configure the following options:
  - For Name, accept the default.
  - For Zone, select **Trust**.
  - For Encapsulation Type, select **mlfr-uni-nni**.
4. Configure MLFR options:
  - For Name, accept the default.

- For Zone, select **Trust**.
5. Click **OK** to save your changes.

#### Related Documentation

- [Setting Interface Properties Using the General Properties Screen on page 53](#)
- [Interface Network Address Translation Methods on page 62](#)
- [Example: Configuring an Aggregate Interface \(NSM Procedure\) on page 77](#)

## Example: Configuring a Loopback Interface (NSM Procedure)

A loopback interface emulates a physical interface on a security device. However, unlike a physical interface, a loopback interface is always in the up state as long as the device on which it resides is up. You might want to use a loopback interface as:

- The management interface—You can manage the device using either the IP address of a loopback interface or the manage IP address that you assign to a loopback interface.
- A virtual security interface (VSIs) for NSRP—The physical state of the VSI on the loopback interface is always up. The interface can be active or not, depending upon the state of the VSD group to which the interface belongs.
- A source interface for specific traffic (such as syslog packets) that originates from the device—When you define a source interface for an application, the specified source interface address is used instead of the outbound interface address to communicate with an external device.

Loopback interfaces are named `loopback.id_num`, where `id_num` is a number greater than or equal to 1 (the maximum `id_num` value you can specify is platform-specific) and denotes a unique loopback interface on the device. Like a physical interface, you must assign an IP address to a loopback interface and bind it to a security zone.



**NOTE:** You cannot bind a loopback interface to a HA zone, nor can you configure a loopback interface for Layer 2 operation or as a redundant/aggregate interface. You cannot configure the following features on loopback interfaces: NTP, DNS, VIP, secondary IP, track IP, or WebAuth.

After defining a loopback interface, you can then define other interfaces as members of its group. Traffic can reach a loopback interface if it arrives through one of the interfaces in its group. Any interface type can be a member of a loopback interface group—physical interface, subinterface, tunnel interface, redundant interface, or VSI.

In this example, you create the loopback interface `loopback.1`, bind it to the Untrust zone, and assign the IP address `1.1.1.27/24` to it.

To configure a loopback interface:

1. Add a device.

2. Configure the loopback interface:
  - a. In the device navigation tree, select **Network > Interface**.
  - b. Click the **Add** icon and select **Loopback Interface**. The General Properties screen appears.
  - c. Configure the following:
    - For zone, select **Untrust**.
    - For IP Address/Netmask, enter **1.1.1.27/24**.
    - Ensure that Manageable is enabled.
    - Ensure that the Management IP is 1.1.1.27.
  - d. Click **OK** to save the new interface.
  - e. Click **OK** to save your changes to the device.

**Related Documentation**

- [Setting Interface Properties Using the General Properties Screen on page 53](#)
- [Example: Configuring a Multilink Interface \(NSM Procedure\) on page 78](#)
- [Example: Configuring an Aggregate Interface \(NSM Procedure\) on page 77](#)

---

## Configuring Virtual Security Interfaces

---

Virtual security interfaces (VSIs) are the virtual interfaces that two security devices forming a virtual security device (VSD) share when operating in high availability (HA) mode. Network and VPN traffic use the IP address and virtual MAC address of a VSI. The VSD then maps the traffic to the physical interface, subinterface, or redundant interface to which you have previously bound the VSI. When two security devices are operating in HA mode, you must bind security zone interfaces that you want to provide uninterrupted service in the event of a device failover to one or more VSDs. When you bind an interface to a VSD, the result is a VSI.

For more information about VSIs, see “[NSRP Clusters Overview](#)” on page 361.

**Related Documentation**

- [Setting Interface Properties Using the General Properties Screen on page 53](#)
- [Interface Network Address Translation Methods on page 62](#)
- [Example: Configuring a Loopback Interface \(NSM Procedure\) on page 79](#)

---

## Example: Configuring a Redundant Interface (NSM Procedure)

---

A redundant interface combines two physical interfaces to create one redundant interface, which you can then bind to a security zone. One of the two physical interfaces acts as the primary interface and handles all the traffic directed to the redundant interface; the other physical interface is the secondary interface and stands by. If the primary interface fails, traffic to the redundant interface fails over to the secondary interface, which becomes the new primary interface.

Because redundant interfaces enable failover at the interface level, before a failure escalates to the device failover level, they are often used when deploying two security devices in a high availability configuration (HA). You can use the dedicated physical redundant HA interfaces or bind two generic interfaces to the HA zone (you can also create redundant security zone interfaces). Then, if the link from the primary interface to the switch becomes disconnected, the link fails over to the secondary interface, preventing a device failover from the VSD primary to backup.



**NOTE:** You cannot combine subinterfaces in a redundant interface. However, you can define a VLAN on a redundant interface in the same way that you can define a VLAN on a subinterface.

In this example, devices A and B are members of two VSD groups—VSD group 0 and VSD group 1—in an active/active configuration. Device A is the primary device of VSD group 0 and the backup in VSD group 1. Device B is the primary device of VSD group 1 and the backup in VSD group 0. The devices are linked to two pairs of redundant switches—switches A and B in the Untrust zone, and switches C and D in the Trust zone.

Because devices A and B are members of the same NSRP cluster, device A propagates all interface configurations to device B except the manage IP address, which you enter on the redundant2 interface on both devices. You put ethernet1/1 and ethernet1/2 in redundant1, and ethernet2/1 and ethernet2/2 in redundant2. On the redundant2 interface, you define a manage IP of 10.1.1.21 for device A and a manage IP of 10.1.1.22 for device B on this interface.

The physical interfaces that are bound to the same redundant interface connect to different switches:

- Physical interfaces bound to a redundant interface in the Untrust zone: ethernet1/1 to switch A, ethernet1/2 to switch B.
- Physical interfaces bound to a redundant interface in the Trust zone: ethernet2/1 to switch C, ethernet2/2 to switch D.

By putting ethernet1/1 and ethernet2/1 in their respective redundant interfaces first, you designate them as primary interfaces. If the link to a primary interface becomes disconnected, the device reroutes traffic through the secondary interface to the other switch without requiring the VSD primary device to fail over.

The physical interfaces do not have to be in the same security zone as the redundant interface to which you bind them. IP addresses for multiple VSIs can be in the same subnet or in different subnets if the VSIs are on the same redundant interface, physical interface, or subinterface. If the VSIs are on different interfaces, they must be in different subnets. [Table 25 on page 81](#) lists IP addresses for the VSIs.

**Table 25: VSI IP Addresses**

VSi	IP Address	VSi	IP Address
redundant1	210.1.1.1/24	redundant1:1	210.1.1.2/24

Table 25: VSI IP Addresses (*continued*)

VSi	IP Address	VSi	IP Address
redundant2	10.1.1.1/24	redundant2:1	10.1.1.2/24

In this example, if the cable from ethernet1/1 becomes disconnected, the port fails over to ethernet1/2. Consequently, all the traffic to and from devices A and B passes through switch B. Reconnecting the cable from ethernet1/1 on device A to switch A automatically causes that interface to regain its former priority.

To configure a redundant interface:

1. Add the cluster and member devices:
  - For cluster, specify NetScreen-500 security devices running ScreenOS 5.1.
  - Add member Device A.
  - Add member Device B.
2. Create a VSD definition for the cluster:
  - Double-click the **Office 1 Cluster** to open the cluster configuration.
  - In the cluster navigation tree, select **Members**.
  - In the VSD Definitions area, click the **Add** icon.
  - Enter **2**, and then click **OK** to save the new VSD definition.
3. Configure the cluster network module (slot1):
  - In the cluster navigation tree, select **Network > Slot**.
  - Double-click **slot 1** to display the slot configuration dialog box. For Card Type, select **2 Interfaces (10/100)**.
  - Click **OK** to save the slot configuration. Repeat process to add a new network module for slot 2.
4. Configure the redundant1 interface:
  - In the cluster navigation tree, select **Network > Interface**.
  - Click the **Add** icon and select **Redundant Interface**. The General Properties screen appears.
5. Configure the following options, and then click **OK**:
  - For Zone, select **Untrust**.
  - For IP address/netmask, enter **210.1.1.1/24**.
  - Ensure that Manageable is enabled.
  - Ensure that the Management IP is 210.1.1.1.
6. Add ethernet1/1 as a member of the redundant1 interface:

- In the cluster navigation tree, select **Network > Interface**. Double-click **ethernet1/1**. The General Properties screen appears.
  - Configure the Redundant Interface Group as **redundant1**, and then click **OK** to save your changes.
7. Add ethernet1/2 as a member of the redundant1 interface:
- In the cluster navigation tree, select **Network > Interface**. Double-click **ethernet1/1**. The General Properties screen appears.
  - Configure the Redundant Interface Group as **redundant1**, and then click **OK** to save your changes.
8. Configure the redundant2 interface:
- In the cluster navigation tree, select **Network > Interface**.
  - Click the **Add** icon and select **Redundant Interface**. The General Properties screen appears.
9. Configure the following options, and then click **OK**:
- For Zone, select **Trust**.
  - For IP address/netmask, enter **10.1.1.1/24**.
10. Add ethernet2/1 as a member of the redundant2 interface:
- In the cluster navigation tree, select **Network > Interface**. Double-click **ethernet1/1**. The General Properties screen appears.
  - For Redundant Interface Group, select **redundant2**.
  - Click **OK** to save your changes.
11. Add ethernet2/2 as a member of the redundant2 interface:
- In the cluster navigation tree, select **Network > Interface**. Double-click **ethernet1/1**. The General Properties screen appears.
  - For Redundant Interface Group, select **redundant2**.
  - Click **OK** to save your changes.
12. Add the VSI interface for redundant1:
- In the cluster navigation tree, select **Network > Interfaces**. Click the **Add** icon and select **VSI**. The General Properties screen appears.
13. Configure the following options, and then click **OK**:
- For Name, select **redundant1**, and then select **1** (for VSD Group 1).
  - For IP address/Netmask, enter **210.1.1.2/24**.
  - Ensure that Manageable is enabled.
14. Add the VSI interface for redundant2:

- In the cluster navigation tree, select **Network > Interfaces**. Click the **Add** icon and select **VSI**. The General Properties screen appears.
15. Configure the following options, and then click **OK**:
- For Name, select **redundant2**, then select **1** (for VSD Group 1).
  - For IP address/Netmask, enter **10.1.1.2/24**.
  - Ensure that Manageable is enabled.
  - Click **Apply** to apply your changes to the cluster and propagate the settings to each member device.
16. Configure the Manage IP address for each member device:
- In the cluster navigation tree, select **Members**, and then double-click **Device A**.
  - In the device navigation tree, select **Network > Interfaces**, and then double-click **redundant2**. The General Properties screen appears.
  - For Management IP, enter **10.1.1.21**, and then click **OK** to save your changes.
  - In the cluster navigation tree, select **Members**, and then double-click **Device B**.
  - In the device navigation tree, select **Network > Interfaces**, and then double-click **redundant2**. The General Properties screen appears.
  - For Management IP, enter **10.1.1.22**, and then click **OK** to save your changes.
17. Click **OK** to save your changes to the cluster.

**Related Documentation**

- [Setting Interface Properties Using the General Properties Screen on page 53](#)
- [Interface Network Address Translation Methods on page 62](#)
- [Configuring Virtual Security Interfaces on page 80](#)

---

## Example: Configuring a Subinterface (NSM Procedure)

---

A subinterface, like a physical interface, is a doorway through which traffic enters and exits a security zone. You can logically divide a physical interface into several virtual subinterfaces, each of which borrows the bandwidth it needs from the physical interface. Subinterfaces use names that indicate their physical interface, such as ethernet3/2.1 or ethernet2.1.

You can create three types of subinterfaces:

- None (for ScreenOS 5.0 devices only)—The subinterface does not use VLAN tagging.
- Tagged interface (VLAN)—Using VLAN tagging, the subinterface distinguishes between traffic bound for it from traffic bound for other interfaces. For details on configuring VLAN tagging, see “[Example: Routing Traffic to Vsys Using VLAN IDs \(NSM Procedure\)](#)” on page 252.



- Encapsulated (for ScreenOS 5.1 and later devices only)—Using encapsulation, you can create a PPPoE subinterface that does not use VLAN tagging. PPPoE subinterfaces enable the device to handle multiple PPPoE sessions over one physical interface.



**NOTE:** The number of PPPoE sessions per physical interface is determined by the security device platform. For information about configuring multiple PPPoE instances on one interface, see [“About Configuring PPPoE” on page 135](#).

You can create a subinterface on any physical interface in the root system or virtual system, and you can bind a subinterface to the same zone as its physical interface or to a different zone. However, the IP address of a subinterface must be in a different subnet from the IP addresses of all other physical interfaces and subinterfaces.

In this example, you create a subinterface for the Trust zone in the root system. You configure the subinterface on ethernet1, which is bound to the Trust zone. You bind the subinterface to a user-defined zone named “accounting,” which is in the trust-vr. You assign it subinterface ID 3, IP address 10.2.1.1/24, and VLAN tag ID 3. The interface mode is NAT.

To configure a subinterface:

1. Add a device.
2. Configure a new zone:
  - Double-click the device icon to open the device configuration. In the device navigation tree, select **Network > Zone**.
  - Click the **Add** icon and select **Security Zone**. The General Properties Screen appears.
3. Configure the following options, and then click **OK**:
  - For Name, enter **accounting**.
  - For Virtual Router, select **trust-vr**.
4. Configure the subinterface:
  - In the device navigation tree, select **Network > Interface**.
  - Click the **Add** icon and select **Sub Interface**. The General Properties screen appears.
5. Configure the following options, and then click **OK**:
  - For Name, select **ethernet1**, and then select **3**.
  - For VLAN tag, enter **3**.
  - For Zone, select **accounting**.
  - For IP Address/Netmask, enter **10.2.1.1/24**.
  - Ensure that Manageability is enabled.

- Ensure that the Management IP is 10.2.1.1.
  - For Interface Mode, select **NAT**.
6. Click **OK** to save your changes to the device.

**Related Documentation**

- [Setting Interface Properties Using the General Properties Screen on page 53](#)
- [Interface Network Address Translation Methods on page 62](#)
- [Example: Configuring a Redundant Interface \(NSM Procedure\) on page 80](#)

---

## Example: Configuring a WAN Interface (NSM Procedure)

---

Multilink Frame Relay (MLFR) for a user-to-network interface (UNI) on available devices allow for the creation of one or more permanent virtual circuits (PVCs) within the bundle. You create a PVC by configuring a subinterface to the multilink interface. Each subinterface maps to a PVC, which is identified by a data-link connection identifier (DLCI). Note that each PVC can be associated with a separate security zone; the security zone for each PVC can be different from the security zone assigned to the multilink interface.

In this example, you create a subinterface for the multilink interface and assign it to a security zone. Then assign a Frame Relay DLCI and IP address to the subinterface.

To configure a WAN interface:

1. On an SSG520 device running ScreenOS 5.1, add a multilink interface and assign it to the Trust zone.
2. Add and configure a WAN subinterface:
  - In the device navigation tree, select **Network > Interface**.
  - Click the **Add** icon and select **WAN-Sub Interface**. The General Properties screen appears.
3. Configure the following options, and then click **OK**:
  - For Name, select the multilink interface that you want to assign the subinterface to. The subinterface name consists of the multilink interface name and a subinterface number. For example, if the multilink interface name is ml1, its subinterfaces can be ml1.1 and ml1.2
  - For Zone, select **Trust**.
4. Click **OK** to save your changes to the device.

**Related Documentation**

- [Setting Interface Properties Using the General Properties Screen on page 53](#)
- [Interface Network Address Translation Methods on page 62](#)
- [Example: Configuring a Subinterface \(NSM Procedure\) on page 84](#)

---

## Configuring a Tunnel Interface

---

A tunnel interface is a doorway to a VPN tunnel. VPN traffic enters and exits a VPN tunnel through a tunnel interface. When you bind a tunnel interface to a VPN tunnel, you can use that tunnel interface to route VPN traffic to a specific destination.



**NOTE:** VPN Manager automatically creates the necessary tunnel interfaces for route-based VPNs. The user can set DSCP marking value for the interface. Only Route and Policy and Route-based types support DSCP marking. For device-level VPNs, you can create the tunnel interfaces before or after creating the VPN.

When creating a route-based VPNs you must create a tunnel interface to enable the security device to route VPN traffic. You can bind a route-based VPN tunnel to a tunnel interface that is either numbered (with IP address/netmask) or unnumbered (without IP address/netmask).

- [Using Numbered Tunnel Interfaces on page 87](#)
- [Using Unnumbered Tunnel Interfaces on page 87](#)
- [Configuring Maximum Transmission Unit Size on page 88](#)

### Using Numbered Tunnel Interfaces

When the tunnel interface is numbered, you must give the interface an IP address and bind the tunnel interface to a tunnel zone. Using numbered tunnel interfaces enables you to use NAT services for policy-based VPN tunnels. Assign an IP address to a tunnel interface if you want the interface to support one or more dynamic IP (DIP) pools for source Network Address Translation (NAT-src) and mapped IP (MIP) addresses for destination Network Address Translation (NAT-dst).

You can create a numbered tunnel interface in a security zone or a tunnel zone.

### Using Unnumbered Tunnel Interfaces

When the tunnel interface is unnumbered, you must specify the interface from which the tunnel interface borrows an IP address. The security device uses the borrowed IP address as a source address when the device itself initiates traffic—such as OSPF messages—through the tunnel. Use unnumbered tunnel interfaces when the tunnel interface does not need to support NAT services, and your configuration does not require the tunnel interface to be bound to a tunnel zone.

You can create an unnumbered tunnel interface that borrows the IP address from an interface in the same security zone or from an interface in a different zone, as long as both zones are in the same routing domain. However, you cannot bind the tunnel interface to a tunnel zone.

## Configuring Maximum Transmission Unit Size

The MTU size option is only supported by some security devices. As packets traverse different networks, a networking component sometimes needs to break a packet into smaller pieces (fragments) based upon the maximum transmission unit (MTU) of each network. The networking component for the destination network must then reassemble the received fragments into a packet. Because fragmentation and reassembly can impact network performance, you might want to fragment a packet destined for a VPN tunnel as it passes through the tunnel interface (before the packet is encrypted and/or encapsulated).

For devices running ScreenOS 5.1 and later, you can define an MTU size that controls the size of packets sent through the tunnel. When the tunnel interface receives the packet, it breaks the packet into fragments based on the specified MTU size, encrypts and/or encapsulates each fragment, and then sends the traffic through the tunnel. As these packets (fragments) pass through other networks, they might be small enough that networking components do not need to perform further fragmentation—which reduces the network load and can decrease the time it takes to send VPN traffic. The receiving networking component (security device or external device) must still reassemble the fragments as they exit the other end of the VPN tunnel.

To configure an MTU size for a tunnel interface, in the tunnel interface navigation tree, select **Advanced Properties** and enter a value for MTU Size. By default, the size is set to none (the interface does fragment packets entering a VPN tunnel). The acceptable range is from 800 to 1500.

### Related Documentation

- [Setting Interface Properties Using the General Properties Screen on page 53](#)
- [Interface Network Address Translation Methods on page 62](#)
- [Example: Configuring a WAN Interface \(NSM Procedure\) on page 86](#)

---

## ADSL Interface in ScreenOS Devices

An asymmetric digital subscriber line (ADSL) is a digital subscriber line (DSL) technology that enables existing telephone lines to carry both voice telephone service and high-speed digital transmission. To use ADSL with a security device, you must configure the `adsl1` interface on the NetScreen-5GT ADSL security device (which supports ADSL).

### Related Documentation

- [Setting Interface Properties Using the General Properties Screen on page 53](#)
- [ADSL, ADSL Interface, and ADSL Settings in ScreenOS Devices on page 89](#)

---

## ADSL, ADSL Interface, and ADSL Settings in ScreenOS Devices

---

The following are the topics of ADSL Interface:

- [About ADSL on page 89](#)
- [About the ADSL Interface on page 89](#)
- [ADSL Settings from the Service Provider on page 89](#)

### About ADSL

Traditional telephone lines use analog signals to carry voice service through twisted-pair copper wires. However, when using analog transmission, the service provider can use only a small portion of the available bandwidth. To work around this limitation, the service provider can use digital transmission to access a wider bandwidth on the same media, at the same time. Because the service provider separates analog and digital transmissions, you can use your telephone and connect the Internet with your computer at the same time on the same line.

At the service provider's central office, the digital subscriber line access multiplexer (DSLAM) connects many DSL lines to a high-speed network such as an Asynchronous Transfer Mode (ATM) network. ADSL transmission is *asymmetric* because the rate at which you can send data (the *upstream* rate) is considerably less than the rate at which you can receive data (the *downstream* rate). ADSL is ideal for Internet access because most messages sent to the Internet are small and do not require much upstream bandwidth, while most data received from the Internet require greater downstream bandwidth.

You can use the ADSL port on the NetScreen-5GT ADSL security device to enable Internet access for a network—without adding additional phone lines, and without using an additional ADSL modem. For details on connecting and cabling the NetScreen-5GT ADSL, see the *NetScreen-5GT ADSL User's Guide*.

### About the ADSL Interface

The ADSL interface on the NetScreen-5GT ADSL security device uses ATM as its Transport Layer. The interface supports multiple permanent virtual circuits (PVCs), which are continuously available logical connections to the network, on a single physical line (the `adsl1` interface). You can configure additional virtual circuits on the device by creating subinterfaces (such as `adsl1.1`, `adsl1.2`).

Before you can configure the `adsl1` interface, however, you must obtain the DSLAM configuration details for the ADSL connection from the service provider, as detailed in [“ADSL Settings from the Service Provider” on page 89](#).

### ADSL Settings from the Service Provider

The service provider for ADSL Internet access must provide you with some details about the ADSL connection so you can configure the security device to connect to their servers. Not all service providers use the same implementation of ADSL; you might be given any combination of the ADSL parameters as described in [Table 26 on page 90](#).

Table 26: ADSL Settings

ADSL Parameters	Description
Virtual Path Identifier and Virtual Channel Identifier (VPI/VCI)	The service provider identifies the virtual circuit on the DSLAM.
ATM encapsulation method (Multiplexing mode)	<p>The ADSL interface on the security device supports the following ATM Adaptation Layer 5 (AAL5) encapsulations:</p> <ul style="list-style-type: none"> <li>Virtual circuit (VC)-based multiplexing, in which each protocol is carried over a separate ATM virtual circuit.</li> <li>logical link Control (LLC), which enables several protocols to be carried on the same ATM virtual circuit (default encapsulation method). This is the default option for the adsl1 interface on the NetScreen-5GT ADSL security device.</li> </ul> <p>The service provider must tell you the type of multiplexing used on the ADSL line.</p>
Point-to-Point Protocol (PPP)	<p>A standard protocol for transmitting IP packets over serial point-to-point links, such as an ATM PVC. The security device supports the following methods of transporting PPP packets:</p> <ul style="list-style-type: none"> <li>PPP over Ethernet (PPPoE). RFC 2516 describes the encapsulation of PPP packets over Ethernet. For more information about PPPoE, see <a href="#">“About Configuring PPPoE” on page 135</a>.</li> <li>PPP over AAL5 (PPPoA). RFC 1483 describes the encapsulation of network traffic over AAL5. For more information about PPPoA, see <a href="#">“Configuring a PPPoA Client Instance” on page 141</a>.</li> </ul> <p>If the service provider’s network uses PPPoE or PPPoA, the service provider must give you the username and password for the connection, the authentication method used, and any other protocol-specific parameters.</p>
IP addresses	The service provider might give the network a static IP address or a range of IP addresses. The service provider should also give you the address of the DNS server to use for DNS name and address resolution.
Discrete multitone (DMT)	<p>A method for encoding digital data in an analog signal. By default, the ADSL interface uses Auto Detect mode, in which it automatically negotiates the DMT operating mode with the service provider DSLAM. You can change the mode on the adsl1 interface to force the interface to use only one of the following DMT standards:</p> <ul style="list-style-type: none"> <li>American National Standards Institute (ANSI) T1.413 Issue 2, which supports rates up to 8 Mbps downstream and 1 Mbps upstream.</li> <li>International Telecommunications Union (ITU) G.992.1 (also known as G.dmt), which supports minimum data rates of 6.144 Mbps downstream and 640 kbps upstream.</li> <li>ITU 992.2 (also known as G.lite), which supports up to data rates of 1.536 Mbps downstream and 512 kbps upstream. This standard is also called “splitterless DSL” because you do not have to install a signal splitter on your ADSL line (the service provider’s equipment splits the signal remotely).</li> </ul>

- Related Documentation**
- [Interface Network Address Translation Methods on page 62](#)
  - [ADSL Interface in ScreenOS Devices on page 88](#)

## Determining Physical Ports and Logical Interfaces and Zones Using ScreenOS Devices Port Mode

The port mode of a NetScreen-5GT ADSL device determines the binding of physical ports, logical interfaces, and zones as described in [Table 27 on page 91](#).

**Table 27: Physical Ports, Logical Interfaces, and Zones**

Supported Port Modes	Description
Trust-Untrust port mode (default)	<p>This port mode uses the following default settings:</p> <ul style="list-style-type: none"> <li>• Binds the ADSL port to the adsl1 interface, which is bound to the Untrust zone.</li> <li>• Binds Ethernet ports 1-4 to the ethernet1 interface, which is bound to the Trust zone.</li> </ul>
Home-Work port mode	<p>Creates special Home and Work zones to segregate business and home users, while allowing users in both zones to access the Internet (the Untrust zone) through the ADSL interface. This port mode uses the following default settings:</p> <ul style="list-style-type: none"> <li>• Binds Ethernet ports 1 and 2 to the ethernet1 interface, which is bound to the Work security zone.</li> <li>• Binds Ethernet ports 3 and 4 to the ethernet2 interface, which is bound to the Home security zone.</li> <li>• Permits all traffic from the Work zone to the Untrust zone.</li> <li>• Permits all traffic from the Home zone to the Untrust zone.</li> <li>• Permits all traffic from the Work zone to the Home zone.</li> <li>• Denies all traffic from the Home zone to the Work zone (you cannot remove this policy)</li> </ul> <p>In the Home-Work port mode, you must manage the device from the Work zone. You cannot configure the device from the Home zone, nor can you use any management services on the Home zone interface. The default IP address of ethernet1, the Work zone interface, is 192.168.1.1/24.</p>
Trust-Untrust-DMZ port mode	<p>This port mode uses the following default settings:</p> <ul style="list-style-type: none"> <li>• Binds Ethernet ports 1 and 2 to the ethernet1 interface, which is bound to the Trust security zone.</li> <li>• Binds Ethernet ports 3 and 4 to the ethernet2 interface, which is bound to the DMZ security zone.</li> <li>• Binds the ADSL port to the adsl1 interface, which is bound to the Untrust security zone.</li> </ul> <p><b>NOTE:</b> The Trust/Untrust/DMZ port mode is supported only on the Extended version of the NetScreen-5GT ADSL device.</p>

For all supported port modes, the adsl1 interface is the only interface bound to the Untrust zone by default.

You can change the port mode to use different port, interface, and zone bindings on the device. For more information about port modes, see the “Zones” chapter in the “Fundamentals” volume of the *Concepts & Examples ScreenOS Reference Guide*.

- Related Documentation**
- [Backup Connection Using the Untrusted Ethernet Port in ScreenOS Devices](#) on page 92
  - [Example: Configuring NetScreen5GT Devices to Permit Internal Hosts \(NSM Procedure\)](#) on page 93

---

## Backup Connection Using the Untrusted Ethernet Port in ScreenOS Devices

---

When using ADSL, the adsl1 interface serves as the primary connection to the Internet. However, you can configure a backup connection to the Internet using the Untrusted Ethernet port or the Modem port on the security device.



**NOTE:** You can configure only one backup interface.

To configure the backup interface, bind both the adsl1 and backup interface to the Untrust zone to automatically configure the interface failover. If the ADSL interface becomes unavailable, the security device automatically sends outgoing traffic to the backup interface, which connects to the ISP account. When the ADSL interface is again available, the device automatically sends outgoing traffic to the adsl1 interface.

To configure the serial interface for the modem, you must have the following information:

- Login and password for the account to the dialup service provider



**NOTE:** All passwords handled by NSM are case-sensitive.

- Primary phone connection for dialing into the account
- Modem initialization string

For more information about configuring the serial interface on a security device, see the “Interface Redundancy” chapter in the “High Availability” volume of the *Concepts & Examples ScreenOS Reference Guide*.

For details on configuring the modem and ISP settings for the serial interface in NSM, see “[Example: Configuring Modem Connections \(NSM Procedure\)](#)” on page 142.

- Related Documentation**
- [Example: Configuring NetScreen5GT Devices to Permit Internal Hosts \(NSM Procedure\)](#) on page 93
  - [Example: Configuring NetScreen5GT Devices to Connect to the Web Using the PPPoA and ADSL Interfaces \(NSM Procedure\)](#) on page 94
  - [Example: Configuring NetScreen5GT Devices as a Firewall Using the PPPoE and ADSL Interfaces \(NSM Procedure\)](#) on page 96



## Example: Configuring NetScreen5GT Devices to Permit Internal Hosts (NSM Procedure)

In this example, you configure a NetScreen-5GT ADSL security device to permit internal hosts to access the Internet through the ADSL interface and permit Internet users to access a local Web server while protecting other internal hosts. To segregate traffic flow to the Web server from the rest of the internal network, configure the Web server in the DMZ, and then create a firewall rule that permits HTTP traffic only to the DMZ zone.

To configure a NetScreen-5GT device to permit internal hosts:

1. Add the NetScreen-5GT ADSL security device as ADSL 1 (device name). To enable the DMZ zone, select the Trust/Untrust/DMZ port mode.
2. Configure the adsl1 interface in the Untrust zone:
  - Double-click the device icon to open the device configuration. In the device navigation tree, select **Network > Interface**.
3. Right click the adsl1 interface and select the **Edit** icon. The General Properties screen appears. Using the information you previously obtained from the service provider, configure the following options:
  - For VPI, enter 0; for VCI, enter **35**.
  - For Multiplexing Mode, select **VC Multiplexing**.
  - For IP address/netmask, enter **1.1.1.1/24**.
  - Ensure that Manageable is enabled.
  - Ensure that the Management IP is 1.1.1.1.
  - Ensure that the Mode is NAT.
4. In the interface navigation tree, select **NAT > MIP**. Configure the following options:
  - For Mapped IP, enter **1.1.1.5**.
  - For Netmask, enter **32**.
  - For Host IP, enter **10.1.1.5**.
  - Ensure that the Host Virtual Router is set to **trust-vr**.
5. Click **OK** to add the MIP, and then click **OK** again to save your changes to the ADSL interface.
6. Configure the Trust interface (ethernet1 in the Trust zone).
7. Right-click **ethernet1** and select the **Edit** icon. The General Properties screen appears. Configure the interface to use an IP address and netmask of 192.168.1.1/24. For Interface Mode, select **NAT**.
8. Select the **DHCP Server IP Pools** tab, and then configure the following options:
  - For starting IP, enter **192.168.1.3**.
  - For Value, select **End IP**.

- For ending IP, enter **192.168.1.33**.
9. In the interface navigation tree, select **DHCP**. For DHCP Mode, select **DHCP Server**.
  10. Click **OK** to add the new IP pool, and then click **OK** again to save your changes to the Trust interface.
  11. Configure the DMZ interface (ethernet2 in the DMZ zone).
  12. Double-click **ethernet2**. The General Properties screen appears. Configure the interface to use an IP address and netmask of 10.1.1.1/24. For Interface Mode, select **NAT**.
  13. Click **OK** to save your changes to the DMZ interface, and then click **OK** to save and apply your changes to the device configuration.
  14. Create a Global MIP to reference the MIP you created for the adsl1 interface. You use a Global MIP when configuring NAT in a Security Policy rule; the Global MIP references the MIP for an individual device, enabling you to use one object (the Global MIP object) to represent multiple MIPs in a single rule.
  15. In the navigation tree, select **Object Manager > NAT Objects > MIP**.
  16. Click the **Add** icon to display the new Global MIP dialog box.
  17. Configure the Global MIP.
  18. Create a firewall rule that routes inbound HTTP traffic from any address in the Untrust zone to the MIP host (the Web server) in the DMZ zone. Configure the rule.

**Related Documentation**

- [Example: Configuring NetScreen5GT Devices to Connect to the Web Using the PPPoA and ADSL Interfaces \(NSM Procedure\) on page 94](#)
- [Example: Configuring NetScreen5GT Devices as a Firewall Using the PPPoE and ADSL Interfaces \(NSM Procedure\) on page 96](#)
- [Wireless Interface on ScreenOS Devices Overview on page 99](#)

## Example: Configuring NetScreen5GT Devices to Connect to the Web Using the PPPoA and ADSL Interfaces (NSM Procedure)

---

In this example, you configure a NetScreen-5GT ADSL security device to connect to the Internet using PPPoA and the ADSL interface. The device acts as both a PPPoA client and a DHCP server:

- As a PPPoA client, the device receives the IP address for the ADSL interface. However, the device also receives one or more IP addresses for DNS servers.
- As a DHCP server, the device provides hosts in the Trust zone with their IP addresses and the IP addresses of the DNS servers.

To configure a NetScreen-5GT device to connect to the Web using PPPoA and an ADSL interface:

1. Add the NetScreen-5GT ADSL security device.

- For device name, enter **ADSL PPPoA**.
  - Select **Model Device**.
  - For device platform, select **ns5GTadsl-Trust-Untrust**.
2. Configure the ADSL Interface. In the device navigation tree, select **Network > Interface**. Right-click the ADSL1 interface and select the **Edit** icon. Configure the General Properties tab following options:
    - For VPI, enter **0**; for VCI, enter **35**.
    - For Multiplexing Mode, select **LLC/SNAP Encapsulation**.
    - Ensure that Manageable is enabled and that the Management IP is 0.0.0.0.
    - Ensure that the zone is Untrust and the Mode is Route.
  3. Leave all other defaults and click **OK** to save your changes to the interface.
  4. Configure the Trust interface:
    - Double-click the device icon to open the device configuration. In the device navigation tree, select **Network > Interfaces**.
    - Right-click **ethernet1** and select the **Edit** icon. The General Properties screen appears. Configure the interface to use an IP address and netmask of 192.168.1.1/24. For Interface Mode, select **NAT**.
    - In the interface navigation tree, select **DHCP**. For DHCP Mode, select **DHCP Server**.
  5. Select the **DHCP Server IP Pools** tab, and then configure the following:
    - For starting IP, enter **192.168.1.3**.
    - For Value, select **End IP**.
    - For ending IP, enter **192.168.1.33**.
  6. Click **OK** to add the new IP pool, and then click **OK** again to save your changes to the Trust interface.
  7. Configure the PPPoA instance:
    - In the device navigation tree, select **Network > PPPoA**. Right-click the Trust interface and select the **Edit** icon.
  8. Click the **Add** icon to create a PPPoA instance, and then configure the following options:
    - For PPPoA Instance, enter **poa1**.
    - For Interface, select the **adsl1** interface.
    - For Username, enter **Alex**.

- For Password, enter **tSOCbme4NW5iYPshGxCy67Ww48ngtHC0Bw==**
  - Select **Update DHCP Server**.
9. Leave all other defaults and click **OK** to save the PPPoA instance, and then click **OK** to save the device configuration.

After you have updated the device with the modeled configuration, the device administrator can activate PPPoA on the local network.

- First, the device administrator powers down the NetScreen-5GT ADSL security device and all workstations in the Trust zone, and then powers on just the device. The device makes a PPPoA connection to the DSLAM, and obtains the IP address for the ADSL interface and the IP addresses for the DNS servers.
- Finally, the device administrator powers on the workstations to activate DHCP; the workstations automatically receive the IP address for the DNS server and obtain an IP address for themselves when they attempt a TCP/IP connection.

**Related  
Documentation**

- [Example: Configuring NetScreen5GT Devices as a Firewall Using the PPPoE and ADSL Interfaces \(NSM Procedure\) on page 96](#)
- [Wireless Interface on ScreenOS Devices Overview on page 99](#)
- [Configuring DSCP Options Overview on page 99](#)

---

## Example: Configuring NetScreen5GT Devices as a Firewall Using the PPPoE and ADSL Interfaces (NSM Procedure)

---

In this example, you configure the NetScreen-5GT ADSL security device as a firewall with the primary Internet connection through the ADSL interface using PPPoE and a backup Internet connection through the serial modem port and dialup connection.

To configure a NetScreen-5GT device as a firewall using PPPoE ADSL interface:

1. Add the NetScreen-5GT ADSL security device.
  - For device name, enter **ADSL PPPoE**.
  - Select **Model Device**.
  - For device platform, select **ns5GTadsl-Home-Work**.
2. Configure the ADSL Interface. In the device navigation tree, select **Network > Interface**. Right-click the ADSL1 interface and select the **Edit** icon. Configure the General Properties tab:
  - For VPI, enter **0**; for VCI, enter **35**.

For Multiplexing Mode, select **LLC/SNAP Encapsulation**.

Ensure that the zone is Untrust and the Mode is Route.
3. Leave all other defaults and click **OK** to save your changes to the ADSL interface.

4. Configure the Work interface:
  - Double-click the device icon to open the device configuration. In the device navigation tree, select **Network > Interfaces**.
  - Right-click **ethernet1** and select the **Edit** icon. The General Properties screen appears. Configure the interface to use an IP address and netmask of 192.168.1.1/24. For Interface Mode, select **NAT**.
5. In the interface navigation tree, select **DHCP**. For DHCP Mode, select **DHCP Server**.
6. Select the **DHCP Server IP Pools** tab, and then configure the following options:
  - For starting IP, enter **192.168.1.3**.
  - For Value, select **End IP**.
  - For ending IP, enter **192.168.1.33**.
  - Click **OK** to add the new IP pool, and then click **OK** again to save your changes to the Work interface.
7. Configure the Home interface:
  - Double-click the device icon to open the device configuration. In the device navigation tree, select **Network > Interfaces**.
  - Right-click **ethernet2** and select the **Edit** icon. The General Properties screen appears. Configure the interface to use an IP address and netmask of 192.168.2.1/24. For Interface Mode, select **NAT**.
8. In the interface navigation tree, select **DHCP**. For DHCP Mode, select **DHCP Server**.
9. Select the **DHCP Server IP Pools** tab, and then configure a new DHCP IP Pool:
  - For starting IP, enter **192.168.2.2**.
  - For Value, select **End IP**.
  - For ending IP, enter **192.168.2.5**.
10. Click **OK** to add the new IP pool, then click **OK** again to save your changes to the Home interface.
11. Configure the PPPoE instance:
  - In the device navigation tree, select **Network > PPPoE**. Right-click the Trust interface and select the **Edit** icon.
12. Click the **Add** icon to create a PPPoE instance:
  - For PPPoE Instance, enter **poel**.
  - For Interface, select the **adsl1** interface.
  - For Username, enter **Alex**.
  - For Password, enter **tSOCbme4NW5iYPshGxCy67Ww48ngtHC0Bw==**
  - Select **Update DHCP Server**.

13. Leave all other defaults, and then click **OK** to save the PPPoE instance.
14. Configure the backup interface (the serial interface on the modem port):
  - Double-click the device icon to open the device configuration. In the device navigation tree, select **Network > Interfaces**.
  - Right-click the serial interface and select the **Edit** icon. The General Properties screen appears.
  - For Zone, select **Untrust**.
15. Configure the ISP settings for the serial interface:
  - In the device navigation tree, select **Network > Dial > ISP**.
16. Create an ISP and configure the following:
  - For ISP Name, enter **isp1**.
  - For Login Name, enter **kgreen**.
  - For Password, enter **98765432**.
  - For Primary Number, enter **4085551111**.
  - For Alternative Number, enter **408555222**.
  - Ensure that the Priority is **1**.
17. Click **OK** to save the new ISP.
18. Configure the Modem settings for the serial interface:
  - In the device navigation tree, select **Network > Dial > Modem**.
19. Select the **Modem** tab and configure the following options:
  - For Modem Name, enter **mod1**.
  - For Init String, enter **AT&FS7=255S32=6**
  - Select **Is Active**.
20. Click **OK** to save the new modem settings, and then click **OK** again to save your changes to the device configuration.



**NOTE:** The ISP and Modem settings automatically apply to the serial interface; you do not need to manually assign them to the Modem port.

---

**Related  
Documentation**

- [Example: Configuring NetScreen5GT Devices to Connect to the Web Using the PPPoA and ADSL Interfaces \(NSM Procedure\) on page 94](#)
- [Example: Configuring NetScreen5GT Devices to Permit Internal Hosts \(NSM Procedure\) on page 93](#)

## Wireless Interface on ScreenOS Devices Overview

A wireless interface handles wireless traffic on a NetScreen-5GT Wireless security device that is configured as a wireless access point (WAP). [Table 28 on page 99](#) lists the wireless interfaces that are prebound to security zones.

**Table 28: Wireless Interfaces Prebound to Security Zones**

Wireless1	Wzone1
Wireless2	Trust or Work (binding depends on port mode)
Wireless3	DMZ or Home (binding depends on port mode)
Wireless4	Wzone2 (available only on the NetScreen-5GT Wireless security device with extended license key and extended port mode)

Each wireless interface must use a separate subnet from all other wireless and wired interfaces. To shutdown an interface, select the **Shutdown Interface** option in the General Properties tab for the interface.

To enable the wireless interface to handle wireless traffic, you must associate the interface with a service set identifier (SSID). The SSID links its basic service set (BSS) with the interface, which in turn is prebound to a security zone. Because there can be only one BSS per security zone, the rules you apply to that zone also apply to the BSS in that zone. For details on binding a wireless interface to an SSID, see [“Configuring Wireless General SSID Settings” on page 388](#).

### Related Documentation

- [Configuring DSCP Options Overview on page 99](#)
- [Example: Configuring DIP Groups \(NSM Procedure\) on page 100](#)
- [DNS Server Configuration Using DNS Settings on page 103](#)

## Configuring DSCP Options Overview

The administrator can configure the DiffServ code point (DSCP) value for traffic initiated by a security device. Altogether, the DSCP value can be configured for 12 services, including BGP, OSPF, RIP, RIPng, Telnet, SSH, Web, TFTP, SNMP, syslog, Webtrends, and IKE. The Web service contains the HTTP and HTTPS services.

The DSCP marking for self-initiated traffic is required. These self-initiated packets might be dropped by an intermediate device because of lower priority.

The DSCP value of the BGP and the OSPF packet is set to 48, and for all other services the default value is 0. The value must be in the range of 0 to 63. The priority is lowest when the DSCP value is set to 0.

When the administrator sets the DSCP value for a specific service, the DSCP field of all the self-initiated packets that belong to that service are set to the specified value.

**Related  
Documentation**

- [Example: Configuring DIP Groups \(NSM Procedure\) on page 100](#)
- [DNS Server Configuration Using DNS Settings on page 103](#)
- [Example: Configuring DNS Proxy Entries \(NSM Procedure\) on page 105](#)

---

## Example: Configuring DIP Groups (NSM Procedure)

---

Use a DIP group to combine two DIP pools for two security devices that are in an active/active NRSP configuration. When specifying the NAT settings in the rule options for a Security Policy rule, you can select a DIP group instead of a single DIP pool.

Selecting a DIP group in the policy enables NAT using the DIP pool that exists on either device in the HA configuration. Typically, two security devices in an active/active configuration share the same configuration, and both devices process traffic simultaneously. When you define a policy to perform NAT using a DIP pool located on one VSI, because that VSI is active only on the device acting as the primary device of the VSD group to which the VSI is bound, any traffic sent to the other device—the one acting as the backup of that VSD group—cannot use that DIP pool and is dropped. To solve this problem, you can create two DIP pools—one on the Untrust zone VSI for each VSD group—and combine the two DIP pools into one DIP group, which you reference in the policy. Each VSI uses its own VSD pool even though the policy specifies the DIP group.

If you do not use a DIP group, the security device that acts as the backup of a VSD group cannot use a DIP pool located on the VSI of the primary of the VSD group. For more details about DIP groups on security devices, see the “ Fundamentals” volume in the *Concepts & Examples ScreenOS Reference Guide*.

In this example, you configure a DIP group that includes the DIP pools of two security devices in an active/active NRSP configuration. By combining the DIP pools located on both Untrust zone VSIs (for VSD groups 0 and 1) into one DIP group, Devices A and B can both process traffic matching policy “out-nat,” which references not an interface-specific DIP pool but the shared DIP group.

To configure a DIP group:

1. Create the Cluster.

In the navigation tree, select **Device Manager > Devices**. Click the **Add** icon and select **Cluster**. Configure the cluster as follows:

- Add the following two cluster members to the cluster: NS-208 A, NS-208 B. Choose **Model** when adding each device.
- Configure the untrust interface for VSD group 0.
- In the cluster navigation tree, select **Network > Interface**.



- Double-click **ethernet3** (untrust interface on the NS-208 A). The General Properties screen appears.
  - Configure the IP address as 1.1.1.1 and the Netmask as 24. Leave all other settings as default.
2. Configure the trust interface for VSD group 0.
  3. Enter the DIP ID.
  4. Add multiple DIP ranges for a particular DIP ID:
    - Select the **Multiple DIP Range** check box.
    - Click the **Add** icon to display the New MultiRange of DIP dialog box.
    - Enter the identification range for Rang ID.
    - For Lower IP, enter the same IP address as the subnet interface IP address.
    - For Upper IP, enter the same IP address as the subnet interface IP address.
  5. For Start, enter **1.1.1.20**.
  6. For End, enter **1.1.1.29**.
  7. For Shift From, enter **1.1.1.30**.
  8. Select the **Fixed Port** check box.



**NOTE:** The Fixed Port is enabled by default while adding multiple DIP ranges for a DIP ID.

9. For Extended IP, enter **211.10.1.10**.
10. For Netmask, enter **24**.
11. Select **Incoming NAT**.
12. In the cluster navigation tree, select **Network > Interface**.
13. Double-click **ethernet1** (trust interface on the NS-208 A). The General Properties screen appears.
14. Configure the IP address as 10.1.1.1, and the Netmask as 24. Leave all other settings as default.
15. Click **OK** to save your changes.
16. Configure the untrust interface for VSD group 1:
  - In the cluster navigation tree, select **Network > Interface**.
  - Right-click **ethernet3** and select **New > VSI**.
17. Configure the IP address as 1.1.1.2 and the Netmask as 24. Leave all the default values for all other settings.
18. Select **NAT > DIP** to display the Dynamic IP dialog box. Configure the following options and click **OK**:

19. Enter the DIP ID.
20. Add multiple DIP ranges for a particular DIP ID:
  - Select the **Multiple DIP Range** check box.
  - Click the **Add** icon to display the New MultiRange of DIP dialog box.
  - Enter the identification range for Rang ID.
  - For Lower IP, enter the same IP address as the subnet interface IP address.
  - For Upper IP, enter the same IP address as the subnet interface IP address.
21. For Start, enter **1.1.1.30**.
22. For End, enter **1.1.1.39**.
23. For Shift From, enter **1.1.1.20**.
24. Select the **Fixed Port** check box.



**NOTE:** The Fixed Port is enabled by default while adding multiple DIP range for a DIP ID.

---

25. For Extended IP, enter **211.10.1.10**.
26. For Netmask, enter **24**.
27. Select **Incoming NAT**.
28. Click **OK** to save your changes.
29. Configure the trust interface for VSD group 1.
30. In the cluster navigation tree, select **Network > Interface**.
31. Right-click **ethernet1** and select **New > VSI**.
32. Configure the IP address as 10.1.1.2, and the Netmask as 24. Leave all other settings as default.
33. Click **OK** to save your changes.
34. Create the DIP group:
  - In the cluster navigation tree, select **Network > DIP Group**.
  - Click the **Add** icon in the DIP Group configuration screen. The Dynamic IP dialog box appears.
  - Configure the DIP Group Name as 7, and select DIP members 5 and 6.
  - Click **OK** to close the Dynamic IP dialog box, and then click **OK** to close and save your changes.
  - Select **DIP Translation Stickiness** to ensure that the device assigns the same IP address from a DIP pool to a host for multiple concurrent sessions.
  - In the cluster navigation tree, select **Network > Advanced > DIP**.

- Select **DIP Translation Stickiness**.
- Click **OK** to save your changes.

For details on DIP Translation Stickiness, see [“Example: Configuring DIP Groups \(NSM Procedure\)” on page 100](#).

35. Create a Global DIP to reference the DIP group for the cluster. You use a Global DIP when configuring NAT in a firewall rule; the Global DIP references the DIP pool or DIP group for an individual device or cluster, enabling you to use one object (the Global DIP object) to represent multiple DIP pools or DIP groups in a single rule.

- In the navigation tree, select **Object Manager > NAT Objects > DIP**.
- Click the **Add** icon to display the new Global DIP dialog box.
- Configure the Global DIP.
- Click **OK** to save your changes.

36. Configure a firewall rule to use the Global DIP object for NAT translation.

#### Related Documentation

- [DNS Server Configuration Using DNS Settings on page 103](#)
- [Example: Configuring DNS Proxy Entries \(NSM Procedure\) on page 105](#)
- [Example: Configuring DDNS Settings \(NSM Procedure\) on page 106](#)

## DNS Server Configuration Using DNS Settings

Use the DNS option to configure DNS server information. Before the security device can use DNS for domain name/address resolution, you must configure the address for the primary DNS server that the device should use.

- [Configuring DNS Settings on page 103](#)
- [Configuring DNS Proxy on page 104](#)

### Configuring DNS Settings

Specify the IP addresses for a Primary DNS server, Secondary DNS server, Tertiary DNS Server, Static Host, and specify refresh interval. You can configure the device to refresh all the entries in its DNS table by checking them with a specified DNS server at a specific time of day at regularly scheduled intervals. Alternatively, you can select **Never Refresh** to ensure that the device does not update its DNS table.



**NOTE:** The device automatically attempts to refresh its DNS table after an HA failover occurs.

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

## Configuring DNS Proxy

Use a DNS proxy to enable split DNS queries. The proxy selectively redirects the DNS queries to specific DNS servers according to partial or complete domain names. This is useful when VPN tunnels or PPPoE virtual links provide multiple network connectivity, and it is necessary to direct some DNS queries to one network, and other queries to another network.



**NOTE:** You can configure DNS proxy for the root device in a vsys, but not for the individual vsys devices.

You can use DNS proxies to make domain lookups more efficient. For example, to reduce load on the corporate server, you can route DNS queries meant for the corporate domain to the corporate DNS server, while routing other DNS queries to the ISP DNS server. You can also use DNS proxy to transmit selected DNS queries through a tunnel interface, preventing malicious users from learning about internal network configuration.

To use a DNS proxy, perform the following:

- Select DNS proxy on the device in the DNS Setting screen.  
The Proxy screen is displayed.
- Select DNS Proxy Instances in the DNS Proxy screen.
- Select **Enable** in the DNS Proxy screen and set the following options:
  - Domain Name
  - Outgoing Interface
  - Primary Server
  - Secondary Server
  - Tertiary Server
  - Failover



**NOTE:** To configure a DNS proxy to use a default DNS server, set the domain name as the asterisk character (\*) for the default DNS proxy, and then select the “failover” option for all nondefault DNS proxies.

### Related Documentation

- [Example: Configuring DNS Proxy Entries \(NSM Procedure\) on page 105](#)
- [Example: Configuring DDNS Settings \(NSM Procedure\) on page 106](#)
- [Advanced Network Settings Overview on page 108](#)

## Example: Configuring DNS Proxy Entries (NSM Procedure)

In this example, you create two DNS proxy entries that selectively forward DNS queries to different servers:

- A DNS query with a FQDN containing the domain name `acme.com` goes out tunnel interface `tunnel.1` to the corporate DNS server at `2.1.1.21`. When a host sends a DNS query to `www.acme.com`, the device automatically directs the query to this server, which resolves the query to `3.1.1.2`.
- A DNS query with a FQDN containing the domain name `acme_eng.com` goes out tunnel interface `tunnel.1` to the DNS server at `2.1.1.34`. When a host sends a DNS query to the `intranet.acme_eng.com`, the device directs the query to this server, which resolves the query to `3.1.1.5`.
- All other DNS queries bypass the corporate servers and go out interface `ethernet3` to the DNS server at `1.1.1.23`. When the host and domain name is `www.juniper.net`, the device automatically bypasses the corporate servers and directs the query to this server, which resolves the query to `207.17.137.68`.

To configure a DNS proxy entry:

1. Add a NS-208 security device running ScreenOS 5.1.
2. In the main navigation tree, select **Device Manager > Devices**, and then double-click the device to open the device configuration.
3. Add the `tunnel.1` interface:
4. In the device navigation tree, select **Network > Interface**.
5. Click the **Add** icon and select tunnel interface.
6. Click **OK** to save the new interface.
7. Configure the Trust interface:
  - In the device navigation tree, select **Network > Interface**.
  - Double-click the trust interface. The General Properties screen appears.
  - Select **Enable DNS Proxy**.
  - Click **OK** to save the new interface.
8. Configure general DNS proxy settings:
  - In the device navigation tree, select **Network > DNS > DNS Proxy**.
  - Select **Configure DNS Proxy Instance**.
  - Select **Enable**.
9. Add the DNS proxy for `acme.com`:
  - Click the **Add** icon. The New DNS Proxy dialog box appears.
10. Configure the following options, and then click **OK**:

- For Domain Name, enter **acme.com**.
  - For Outgoing Interface, enter **tunnel.1**
  - For Primary DNS Server, enter **2.1.1.21**.
  - Select **Failover**.
  - Add the DNS proxy for acme\_eng.com:
  - Click the **Add** icon. The New DNS Proxy dialog box appears.
11. Configure the following options, and then click **OK**:
- For Domain Name, enter **.acme\_eng.com**.
  - For Outgoing Interface, enter **tunnel.1**.
  - For Primary DNS Server, enter **2.1.1.34**.
  - Select **Failover**.
  - Add the DNS proxy for all other DNS requests:
  - Click the **Add** icon. The New DNS Proxy dialog box appears.
12. Configure the following options:
- For Domain Name, enter **\***.
  - For Outgoing Interface, enter **ethernet3**
  - For Primary DNS Server, enter **1.1.1.23**.
13. Click **OK** to save your changes to the device.

**Related Documentation**

- [Example: Configuring DDNS Settings \(NSM Procedure\) on page 106](#)
- [Advanced Network Settings Overview on page 108](#)

---

## Example: Configuring DDNS Settings (NSM Procedure)

---

Use Dynamic DNS (DDNS) to enable client devices to dynamically update IP addresses for registered domain names. You might want to use DDNS for a security device that dynamically receives its IP address from an ISP through PPP, DHCP, or XAuth. When the device is protecting a Web server, clients from the Internet can access that Web server using a domain name, even if the IP address of the security device changes.



**NOTE:** You can configure Dynamic DDNS for the root device in a vsys, but not for the individual vsys devices.

A DDNS server stores dynamically changed addresses and associated domain names. It also supports custom and static service types on a device running ScreenOS 6.1 or later. To use DDNS, you must set up an account, including username and password, with the DDNS server, such as dyndns.org or ddo.jp. The security device updates DDNS servers

with the account information periodically, or in response to IP address changes, and the DDNS server uses the account information to configure client devices.

To control how often the device updates the DDNS server, set the number of minutes between DDNS updates. The default (and recommended) value is 60 minutes; accepted range is 1-1440. However, the device might not update at every interval because the DNS server must first time out the DDNS entry from its cache. If you set the Minimum Update Interval too low, the security device may lock you out.

In this example, you configure a security device to use the DDNS server [dyndns.org](http://dyndns.org) for resolving changed addresses. In the DDNS settings, you define the Web server as the protected host, and then bind the host to the source interface (ethernet3). When the device sends an update to the ddo.jp server, the host name ([www.my.host.com](http://www.my.host.com)) is associated with the interface (ethernet3).

To configure DDNS settings:

1. Add a NetScreen-208 security device running ScreenOS 5.1.
2. In the main navigation tree, select **Device Manager > Devices**, and then double-click the device to open the device configuration.
3. Configure general dynamic DNS settings:
  - In the device navigation tree, select **Network > DNS > Dynamic DNS**.
  - Select **Configure Dynamic DNS Instance**.
  - Select **Enable Dynamic DNS**.
4. Add the DDNS instance for the Web server:
  - Click the **Add** icon. The New Dynamic DNS dialog box appears.
5. Configure the following options:
  - For ID, enter **12**
  - For Server Type, select **dyndns**.
  - For FQDN Server Name, enter **dyndns.org**.
  - For Service Type, enter **static dns service**.
  - For Refresh Interval (Hours), enter **24**.
  - For Minimum Update Interval (Minutes), enter **15**.
  - For User Name of DDNS Account, enter **swordfish**.
  - For Password for DDNS Account, enter **ad93lxb**.



**NOTE:** You do not need to enter an agent name. The security device automatically generates the agent name using internal information, such as the ScreenOS version, serial name, and platform.

- For Source Interface, select **ethernet3**.
  - For Host Name, enter **www.my\_host.com**.
6. Click **OK** to save the new DDNS instance, and then click **OK** to save your changes to the device.

**Related  
Documentation**

- [Example: Configuring DNS Proxy Entries \(NSM Procedure\) on page 105](#)
- [Advanced Network Settings Overview on page 108](#)

---

## Advanced Network Settings Overview

In the Advanced Network screens, you can configure the following network settings:

- [Configuring ARP Cache Entries on page 108](#)
- [Configuring VIP Options on page 108](#)
- [Configuring DIP Options on page 109](#)

### Configuring ARP Cache Entries

Use the ARP option to manually add entries to the Address Resolution Protocol (ARP) cache. The ARP cache contains associations of IP addresses to physical machine addresses known as media access control (MAC) addresses. The ARP normally resolves unknown IP addresses and updates its cache automatically. You can manually add ARP cache entries, if necessary, for testing or troubleshooting purposes.

To add an ARP cache entry:

1. Click the **Add** icon in the ARP configuration screen.
2. Specify the IP address, interface, and MAC address for the ARP entry.
3. Click **OK**.

For more detailed explanation about configuring ARP entries on security devices, see the **arp** commands in the *NetScreen CLI Reference Guide*.

### Configuring VIP Options

A virtual IP (VIP) address maps traffic received at one IP address to another address based on the destination port number in the TCP or UDP segment header. You can only set a VIP on an interface in the Untrust zone. The IP address for the VIP must be in the same subnet as an interface in the Untrust zone. (On some security devices, the IP address for the VIP can be the same address as the Untrust zone interface.) In addition, you need the following information to define a VIP:

- The IP addresses for the servers that process the requests
- The type of service you want the security device to forward from the VIP to the IP address of the host



Use the VIP Options configuration screen to set multiple port entries for VIPs. A single VIP can support custom services with multiple port entries by creating multiple service entries under that VIP. To use multiple-port services in a VIP, you need to enable multiple port services, and then reset the security device.

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

## Configuring DIP Options

Use DIP Options to set DIP translation operation.

When DIP is configured on an interface, the security device normally assigns a different source IP address for each session, even when a single host initiates several sessions that require NAT using the DIP pool. This random address assignment can be problematic for services that create multiple sessions that require the same source IP address for each session.

For example, it is important to have the same IP address for multiple sessions when using the AOL Instant Messaging (AIM) client. You create one session when you log in, and another for each chat. For the AIM server to verify that a new chat belongs to an authenticated user, it must match the source IP address of the login session with that of the chat session. If they are different—possibly because they were randomly assigned from a DIP pool during the NAT process—the AIM server rejects the chat session.

To ensure that the device assigns the same IP address from a DIP pool to a host for multiple concurrent sessions, select DIP Translation Stickiness.

For more detailed explanation about configuring DIP options on security devices, see the “Fundamentals” volume in the *Concepts & Examples ScreenOS Reference Guide*.

For details about creating a DIP group, see [“Example: Configuring DIP Groups \(NSM Procedure\)” on page 100](#).

### Related Documentation

- [Example: Configuring DDNS Settings \(NSM Procedure\) on page 106](#)
- [Example: Configuring DNS Proxy Entries \(NSM Procedure\) on page 105](#)



## CHAPTER 4

# Advanced Network Settings

This chapter details the advanced network setting options for the managed device. For instructions on configuring specific device settings, see the *Network and Security Manager Online Help*.

This chapter contains the following topics:

- [Configuring Advanced Device Settings Overview on page 112](#)
- [Example: Defining Forced Timeout \(NSM Procedure\) on page 112](#)
- [Identifying Reasons for Session Close in NSM on page 113](#)
- [Configuring Policy Schedules \(NSM Procedure\) on page 114](#)
- [Configuring Timeouts for Predefined Services \(NSM Procedure\) on page 115](#)
- [Configuring Session Cache for Predefined Services \(NSM Procedure\) on page 115](#)
- [Configuring SIP Settings on page 116](#)
- [Configuring MGCP Settings on page 118](#)
- [Configuring H.323 Settings on page 119](#)
- [Allocating Network Bandwidth Using Traffic Shaping Options on page 119](#)
- [Enabling/Disabling Application Layer Gateway Protocols Overview on page 121](#)
- [Using Packet Flow Options on page 122](#)
- [Configuring Features Unsupported in NSM Using Supplemental CLI Options Overview on page 129](#)
- [Configuring ScreenOS with TFTP or FTP Servers Enabled Using TFTP/FTP Options on page 130](#)
- [Configuring Hostnames and Domain Names Overview on page 130](#)
- [Configuring NSGP Overview on page 131](#)
- [NSGP Modules Overview on page 131](#)
- [Example: Configuring NSGP on GTP and Gi Firewalls \(NSM Procedure\) on page 132](#)
- [Using the PPP Option to Configure Point-To-Point Protocol Connections on page 134](#)
- [About Configuring PPPoE on page 135](#)
- [Example: Updating DNS Servers \(NSM Procedure\) on page 136](#)
- [Example: Configuring Multiple PPPoE Sessions on a Single Interface \(NSM Procedure\) on page 138](#)

- [Configuring a PPPoA Client Instance on page 141](#)
- [Configuring a NetScreen Address Change Notification on page 141](#)
- [Interface Failover in ScreenOS Devices on page 141](#)
- [Example: Configuring Modem Connections \(NSM Procedure\) on page 142](#)
- [Example: Creating Modem Settings \(NSM Procedure\) on page 143](#)
- [Example: Creating ISP Connection Settings \(NSM Procedure\) on page 143](#)
- [Setting ISP Priority for Failover on page 144](#)

## Configuring Advanced Device Settings Overview

---

Use the advanced screens to configure advanced options for the security device. In the device navigation tree, select **Advanced** to view configuration options.

The following are the different settings that details the advanced options for security devices:

- Timeouts for Predefined Services
- SIP Settings
- MGCP Settings
- H.323 Settings
- Traffic Shaping
- Application Layer Gateways (ALGs)
- Packet Flow
- Supplemental Command Line Interface (CLI)
- TFTP/FTP Server Operation
- Host and Domain Name
- NSGP

### Related Documentation

- [Example: Defining Forced Timeout \(NSM Procedure\) on page 112](#)
- [Identifying Reasons for Session Close in NSM on page 113](#)
- [Configuring Policy Schedules \(NSM Procedure\) on page 114](#)

## Example: Defining Forced Timeout (NSM Procedure)

---

Forced timeout, unlike idle timeout, does not depend on the idleness of the user, but on an absolute timeout after which access for the authenticated user is terminated. The authentication table entry for the user is removed, as are all associated sessions for the authentication table entry. The default is 0 (disabled), and the range is 0 to 10000 (6.9 days).

In the following example, if you change the authentication idle timeout value from the default (10 minutes) to 30 minutes and the RADIUS retry timeout from 3 seconds to 4 seconds, the session could theoretically remain open indefinitely (as long as one keystroke is sent every 30 minutes). You can limit total session time by setting forced-timeout to 60 minutes. With this setting, after one hour the authentication table entry for the user is removed, as are all associated sessions for the authentication table entry, and the user needs to reauthenticate.



**NOTE:** For detailed information on changing authentication server settings, see *Concepts & Examples ScreenOS Reference Guide*.

To define forced timeout:

1. In the NSM navigation tree, select **Device Manager>Security Devices**.
2. Select a security device and then double-click the device on which you want to define forced timeout. The device configuration appears.
3. In the device navigation tree, select **Auth>Default Servers**.
4. Specify a valid range in minutes for the Local Auth Server Timeout.
5. Specify a valid range in minutes for the Local Auth Server Forced Timeout.
6. Click **OK** to apply your settings.

**Related Documentation**

- [Identifying Reasons for Session Close in NSM on page 113](#)
- [Configuring Policy Schedules \(NSM Procedure\) on page 114](#)
- [Configuring Advanced Device Settings Overview on page 112](#)

## Identifying Reasons for Session Close in NSM

NSM supports the log reason for the session close feature. NSM displays the reason for session close so that you can differentiate session creation messages from session close messages. If you do not want the reason to display, you can explicitly configure the device not to display the field. [Table 29 on page 113](#) lists the reasons for session close that NSM identifies. Any session that cannot be identified is labeled OTHER.

**Table 29: Session Closings**

TCP FIN	TCP connection torn down because of FIN packet.
TCP RST	TCP connection torn down because of RST packet.
RESP	Special sessions, such as PING and DNS, close when response is received.
ICMP	ICMP error received.
AGE OUT	Connection aged out normally.

Table 29: Session Closings (*continued*)

ALG	ALG forced session close either because of error or other reasons specific to that ALG.
NSRP	NSRP session close message received.
AUTH	Session closed because of authentication failure.
OTHER	Reason for close not identified.

**Related  
Documentation**

- [Configuring Policy Schedules \(NSM Procedure\) on page 114](#)
- [Configuring Timeouts for Predefined Services \(NSM Procedure\) on page 115](#)
- [Example: Defining Forced Timeout \(NSM Procedure\) on page 112](#)

## Configuring Policy Schedules (NSM Procedure)

By associating a schedule to a policy, you can determine when the policy is in effect. You can configure schedules on a recurring basis and as a one-time event. Schedules provide a powerful tool in controlling the flow of network traffic and in enforcing network security. For an example of the latter, if you were concerned about employees transmitting important data outside the company, you might set a policy that blocked outbound FTP-Put and MAIL traffic after normal business hours.



**NOTE:** In the Web UI, scheduled policies appear with a gray background to indicate that the current time is not within the defined schedule. When a scheduled policy becomes active, it appears with a white background.

To configure a policy schedule:

1. In the NSM navigation tree, select **Object Manager>Schedule Objects**.
2. Click **New** and fill in the schedule form.
3. Click **OK** to save the schedule.

You can attach a schedule to a policy as you create the policy, or you can bind the schedule later in the Web UI. For more information on policies and schedules, see the *Network and Security Manager Administration Guide* and the *Concepts & Examples ScreenOS Reference Guide*.

**Related  
Documentation**

- [Configuring Timeouts for Predefined Services \(NSM Procedure\) on page 115](#)
- [Configuring Session Cache for Predefined Services \(NSM Procedure\) on page 115](#)
- [Identifying Reasons for Session Close in NSM on page 113](#)

## Configuring Timeouts for Predefined Services (NSM Procedure)

Use the Predefined Service Timeout option to configure timeouts for predefined services. Services are types of IP traffic for which protocol standards exist. Each service has a port number associated with it, where the access policy accepts a request for that service. When you create an access policy, you must define a service for it. You can select one of the predefined services or select a custom service that you have created. For predefined services, you can use the default timeout specified by the protocol or you can configure a different timeout value.

To configure a timeout for a predefined service:

1. Click the **Add** icon in the Predefined Service Timeout configuration screen. The Predefined Service Timeout dialog box appears.
2. Select the service from the Name list.
3. Select **User-defined Value** from the Timeout list.
4. Enter the timeout value.
5. Click **OK**.

For more information about configuring timeouts for predefined services on security devices, see the “Fundamentals” volume in the *Concepts & Examples ScreenOS Reference Guide*.



**NOTE:** For security devices running ScreenOS 5.2 and later, you can also configure predefined service timeouts on virtual systems.

### Related Documentation

- [Configuring Session Cache for Predefined Services \(NSM Procedure\) on page 115](#)
- [Configuring Policy Schedules \(NSM Procedure\) on page 114](#)

## Configuring Session Cache for Predefined Services (NSM Procedure)

Use the Predefined Service Session Cache option to configure the session cache for predefined services. You can also set the total session cache number.

To configure a session cache for a predefined service:

1. Double-click the device to open the device configuration.
2. In the device navigation tree, select **Advanced > Pre-defined Service Session Cache**. The Pre-defined Service Session Cache screen appears.
3. Select the **Enable session cache** check box.
4. Select a number from the Total session cache number field.
5. Click **Add**. The New Pre-defined Service Session cache dialog box appears.



**NOTE:** All predefined services will be displayed in the dialog box. Click **Edit Pre-defined Service**. (The **New** button is grayed out on root device).

6. Select a name from the **Name** drop-down list.
7. Select the **Enable session cache for service** check box.
8. Click **OK** to create a predefined service session cache.
9. Click **OK** to save your changes.

**Related  
Documentation**

- [Configuring SIP Settings on page 116](#)
- [Configuring Timeouts for Predefined Services \(NSM Procedure\) on page 115](#)
- [Configuring MGCP Settings on page 118](#)

---

## Configuring SIP Settings

Use the SIP Settings option to configure Session Initiation Protocol (SIP) as a service on the security device. SIP is an Internet Engineering Task Force (IETF)-standard protocol for initiating, modifying, and terminating multimedia sessions (such as conferencing, telephony, or multimedia) over the Internet. SIP is used to distribute the session description, to negotiate and modify the parameters of an existing session, and to terminate a multimedia session.

The device can then screen SIP traffic, permitting or denying it based on a security policy that you configure. SIP is a predefined service in ScreenOS and uses port 5060 as the destination port. Security devices currently do not support NAT (network address translation) with SIP.

SIP is used to distribute the session description and, during the session, to negotiate and modify the parameters of the session. SIP is also used to terminate the session.

SIP messages consist of requests from client to server and responses to requests from servers to clients with the purpose of establishing a session (or a call). A UA (user agent) is an application that runs at the endpoints of the call and consists of two parts: the UAC (user agent client) that sends SIP requests on behalf of the user, and a UAS (user agent server) who listens to the responses and notifies the user when they arrive. Examples of user agents are SIP proxy servers and SIP phones.

A call can have one or more voice channels. Each voice channel has two sessions (or two media streams), one for RTP and one for RTCP. When managing the sessions, the security device considers the sessions in each voice channel as one group. Settings such as the inactivity timeout apply to a group as opposed to each session.

### Setting SIP Inactivity Timeouts

You can configure the following types of inactivity timeouts that determine the lifetime of a group:



- **Signaling Inactivity Timeout**—This parameter indicates the maximum length of time (in seconds) a call can remain active without any SIP signaling traffic. Each time a SIP signaling message occurs within a call, this timeout resets. The default setting is 43,200 seconds (12 hours).
- **Media Inactivity Timeout**—This parameter indicates the maximum length of time (in seconds) a call can remain active without any media (RTP or RTCP) traffic within a group. Each time a RTP or RTCP packet occurs within a call, this timeout resets. The default setting is 120 seconds.

If either of these timeouts expire, the security device removes all sessions for this call from its table, thus terminating the call.

Select any of the appropriate check boxes to pass messages that cannot be decoded by the device in either Route mode or NAT mode:

- Pass nonparsable packets in Route mode
- Pass nonparsable packets in NAT mode

### Configuring SIP Firewall Features

Multiple SIP INVITE requests can overwhelm a SIP proxy server. You can configure the security device to monitor INVITE requests (and the proxy server replies) to protect SIP proxy servers.

- **SIP Attack Protection**—To drop multiple, identical SIP INVITE messages, configure SIP Attack Protection and enter the number of seconds for which you want to drop similar packets. If SIP proxy server reply contains a 3xx, 4xx, or 5xx response code, the ALG stores the source IP address of the request and the IP address of the proxy server in a table. The security device checks all INVITE requests against this table and discards matching packets for the specified number of seconds.
- **Destination IP Server Protection**—To protect a specific SIP proxy server from multiple identical SIP INVITE requests, configure Destination IP Server Protection for a specific IP address and netmask.
  - If you do not specify a specific SIP proxy server, SIP Attack Protection monitors all SIP traffic for multiple identical SIP INVITE messages.
  - If you do specify a specific SIP proxy server, SIP Attack Protection monitors only SIP traffic destined for the specified SIP proxy server.

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

#### Related Documentation

- [Configuring Timeouts for Predefined Services \(NSM Procedure\) on page 115](#)
- [Configuring MGCP Settings on page 118](#)
- [Configuring Session Cache for Predefined Services \(NSM Procedure\) on page 115](#)

## Configuring MGCP Settings

---

To configure Media Gateway Control Protocol (MGCP), use the MGCP Settings option. MGCP is a text-based, Application Layer protocol that can be used for call setup and call control. The protocol is based on a master/slave call control architecture: the media gateway controller (call agent) maintains call control intelligence, and media gateways carry out the instructions from the call agent.

### Setting MGCP Inactivity Timeouts

You can configure the following types of inactivity timeouts that determine the lifetime of a group:

- Inactive Media Timeout in seconds—This parameter indicates the range a call can remain inactive without any MGCP traffic. Each time an MGCP message occurs within a call, this timeout resets. If the timeout value is reached, the security device removes all sessions for this call from its table, thus terminating the call. The default setting is 120 seconds and the range of values is 10 to 255 seconds.
- Transaction Timeout in seconds—This parameter indicates the range of time a call can remain inactive between the gateway and the certificate authority (CA). If the timeout value is reached, the security device removes all sessions for this call from its table, thus terminating the call. The default setting is 30 seconds and the available values range from 5 to 50 seconds.
- Maximum call duration in minutes—This parameter indicates the maximum length of time a call can remain inactive between the gateway and the certificate authority (CA). The call is cleared if the transaction times out. The default is 720 minutes.

As a firewall, it might be necessary to parse all messages strictly and drop the unidentified messages. However, the following options are available to pass messages that cannot be decoded by the device in either Route mode or NAT mode:

- Pass unidentified MGCP message in route mode
- Pass unidentified MGCP message in NAT mode

### Configuring MGCP Firewall Features

The MGCP firewall features allow you to enable flood protection to and from the gateway.

- Connection Flood Protection to/from Gateway—Control pinhole connections by setting a limit to the rate of CRCX command processing. CRCX commands that exceed the limit are dropped. The range is 1 to 65,535 and the default is 1,000.
- Message Flood Protection to/from Gateway—Messages are dropped if they arrive at a rate (in seconds) higher than the configured rate. The range is 1 to 200 and the default is 200 seconds.

For more information about configuring MGCP on security devices, see the “Fundamentals” volume in the *Concepts & Examples ScreenOS Reference Guide*.

- Related Documentation**
- [Configuring Session Cache for Predefined Services \(NSM Procedure\) on page 115](#)
  - [Configuring Timeouts for Predefined Services \(NSM Procedure\) on page 115](#)
  - [Configuring SIP Settings on page 116](#)

---

## Configuring H.323 Settings

H.323 Application Layer Gateway (ALG) lets you to secure voice-over-IP (VoIP) communication between terminal hosts, such as IP phones and multimedia devices. In such a telephony system, gatekeeper devices manage call registration, admission, and call status for VoIP calls. Gatekeepers can reside in the two different zones or in the same zone.

The H.323 protocol ALG is enhanced to support incoming calls in NAT mode and slow start in gatekeeper routed mode. In gatekeeper routed mode, all control channel negotiations (Q.931 and H.245) are performed between the gatekeeper and the end points. The media channels, on the other hand, are opened directly between the end points.

### Setting H.323 Inactivity Timeouts

When you enable H.323, the gateway is registered to the flow and reassembly. In addition, the port is also registered. If you do not enable H.323, none are registered. You can configure the following inactivity timeout to determine the lifetime of a group:

- Set incoming-table timeout value—Sets or resets the default timeout value (in seconds) for the NAT table entry. The default value is 3,600 seconds (60 minutes).

Select any of the appropriate check boxes to pass messages that cannot be decoded by the device in either Route mode or NAT mode:

- Pass nonparsable packets in Route mode
- Pass nonparsable packets in NAT mode

For more detailed explanation about configuring H.323 on security devices, see the “Fundamentals” volume in the *Concepts & Examples ScreenOS Reference Guide*.

- Related Documentation**
- [Configuring Session Cache for Predefined Services \(NSM Procedure\) on page 115](#)
  - [Configuring MGCP Settings on page 118](#)
  - [Configuring SIP Settings on page 116](#)

---

## Allocating Network Bandwidth Using Traffic Shaping Options

Use the traffic shaping option to allocate an appropriate amount of network bandwidth to every user and application on a specific device interface. The appropriate amount of bandwidth is defined as cost-effective carrying capacity at a guaranteed quality of service (QoS). To classify traffic, you create security policies and specify the amount of guaranteed bandwidth and maximum bandwidth, and the priority for each class of traffic.

You can also shape traffic at the policy level to allocate bandwidth for particular types of traffic.

Guaranteed bandwidth and maximum bandwidth are not strictly policy based but, with multiple physical interfaces in the egress zone, are based on both policy and total egress physical interface bandwidth available. The physical bandwidth of every interface is allocated to the guaranteed bandwidth parameter for all policies. If there is any bandwidth left over, it is sharable by any other traffic. In other words, each policy gets its guaranteed bandwidth and shares whatever is left over, on a priority basis (up to the limit of its maximum bandwidth specification), with all other policies. Refer to [“Setting Physical Link Attributes for Interfaces” on page 55](#) for more information describing how to configure physical settings on the device interface.

Using the traffic shaping option, you can configure the following traffic shaping parameters:

- **Priority Levels**—You can use the Traffic Shaping screen to perform priority queuing on bandwidth that is not allocated to guaranteed bandwidth, or unused guaranteed bandwidth. Queuing allows the security device to buffer traffic in up to eight different priority queues. The security device maps the eight priority levels to the first three bits in the DiffServ field, or to the IP precedence field in the ToS byte in the IP packet header. By default, the highest priority (priority 0) on the security device maps to 111 in the IP precedence field. The lowest priority (priority 7) maps to 000 in the IP precedence field.
- **Traffic Shaping Mode**—Traffic shaping is automatically determined by the device, but you can set it to on or off.
- **Clear DSCP Class Selector**—The class selector controls the number of bits affected in the DiffServ field. By default, the priority levels affect only the first three bits in the eight bit DiffServ field. The remaining bits are untouched, but can be altered by an upstream router, which might change the IP priority preference. When the DSCP class selector is enabled, the class selector zeroes the remaining five bits in the DiffServ field, which prevents upstream routers from altering priority levels.
- **DiffServ code point Group Marking and DSCP Group**—Sometimes the DSCP value is already marked for incoming traffic in a policy. The device does not need to mark the DSCP value again during a policy match. By enabling the **DiffServ code point Group Marking** option, you can avoid repeated marking of DSCP values in a policy. When the **DiffServ code point Group Marking** option is enabled, you can create DSCP Groups. NSM goes through all the DSCP groups in the DSCP Group list to remove repeated marking of the DSCP values.

You can add a new **DSCP Group**, modify or delete an existing group using the **Add**, **Edit** or **Delete** icons. You can create or delete multiple DSCP Group ranges for a single DSCP Group.

For a more detailed explanation about configuring traffic shaping on security devices, see the “Fundamentals” volume in the *Concepts & Examples ScreenOS Reference Guide*.

**Related  
Documentation**

- [Configuring H.323 Settings on page 119](#)
- [Configuring MGCP Settings on page 118](#)

- [Configuring SIP Settings on page 116](#)

## Enabling/Disabling Application Layer Gateway Protocols Overview

Application Layer Gateways (ALGs) manage specific protocols by intercepting traffic as it passes through the security device. After analyzing the traffic, the ALG allocates resources to permit the traffic to pass securely. By default, all ALGs are enabled on a security device. In situations where a security device is receiving an excessive amount of malicious or accidental traffic of a particular type, you might want to disable the associated ALG.

You can enable or disable the following ALG protocols:

- H.323 —Three ALGs handle specific tasks for H.323 traffic. To disable H.323 on the security device, you must disable the following ALGs:
  - H.245 —This ALG is a control signaling protocol used to exchange messages between H.323 endpoints.
  - Q.931 —This ALG is a Layer 3 protocol used for Integrated Services Digital Network (ISDN) call establishment, maintenance, and termination between H.323 endpoints.
  - RAS —The Registration, Admission, and Status (RAS) ALG is used to register, control admission, change bandwidth, check status, and perform disengage procedures between H.323 endpoints and gatekeepers.
- MSRPC —The Microsoft Remote Procedure Call (MS-RPC) ALG enables a program running on one host to call procedures in a program running on another host. Because of the large number of RPC services and the need to broadcast, the transport address of an RPC service is dynamically negotiated based on the service program's universal unique identifier (UUID).
- RTSP —The Real-Time Streaming Protocol (RTSP) controls delivery of one or more synchronized streams of multimedia, such as audio and video.
- SIP —The Session Initiation Protocol (SIP) is an Internet Engineering Task Force (IETF)-standard protocol for initiating, modifying, and terminating multimedia sessions (such as conferencing, telephony, or multimedia) over the Internet. SIP is used to distribute the session description, to negotiate and modify the parameters of an existing session, and to terminate a multimedia session.
- SQL — The SQL ALG handles SQL, a relational database management system.
- SUNRPC — The Sun Remote Procedure Call (SUNRPC) enables a program running on one host to call procedures in a program running on another host. Because of the large number of RPC services and the need to broadcast, the transport address of an RPC service is dynamically negotiated based on the service's program number and version number.
- MGCP — The Media Gateway Control Protocol (MGCP) is supported on security devices in Route, Transparent, and Network Address Translation (NAT) modes. MGCP is a text-based Application Layer protocol used for call setup and control. MGCP is based on a master-slave call control architecture. The media gateway controller (call agent)

maintains call control intelligence, while the media gateways carry out instructions from the call agent.

- PPTP — The Point-to-Point Tunneling Protocol (PPTP) provides IP security at the Network Layer. PPTP consists of a control connection and a data tunnel. The control connection runs over TCP and helps in establishing and disconnecting calls, and the data tunnel handles encapsulated Point-to-Point Protocol (PPP) packets carried over IP.
- SCTP — The Stream Control Transmission Protocol (SCTP) is an IP transport protocol that exists at the same level as UDP and TCP. SCTP currently provides Transport Layer functions to Internet applications. It provides a reliable transport service that supports data transfer across the network, in sequence and without errors. You can configure the security device to perform stateful inspection on all SCTP traffic without performing deep inspection. If you enable stateful inspection of SCTP traffic, the SCTP ALG drops any anomalous SCTP packets.
- Apple-iChat Settings — The Apple iChat ALG provides support for iChat applications by opening pinholes that allow the text, audio, and video calls to pass through devices running ScreenOS 6.1 or later. When you enable the AppleiChat ALG functionality, the device opens pinholes for the configured call-answer-time to establish the iChat audio/video session. The call-answer-time is the duration of time for which the device opens the pinholes for establishing the iChat audio/video session. The default value for call-answer-time is 32 seconds. When this timer expires, the device closes the pinholes. The range for configuring the call-answer-time is 20 to 90 seconds. The iChat application fragments the packets it sends to the receiver based on the maximum segment size (MSS) of the receiver. The MSS value depends on the network configuration of the receiver. The fragmented packet is reassembled at the ALG for address translation. By default, the reassembly option is disabled.
- IPsec-NAT Settings — You can set the IPsec-NAT timeout to run ESP with a DIP pool. The default value is 30.

**Related  
Documentation**

- [Configuring H.323 Settings on page 119](#)
- [Using Packet Flow Options on page 122](#)
- [Allocating Network Bandwidth Using Traffic Shaping Options on page 119](#)

---

## Using Packet Flow Options

Use the packet flow options to configure the security device to regulate packet flow.

The following sections detail each packet flow option:

- [ICMP Path MTU Discovery on page 123](#)
- [Allow DNS Reply Without Matched Request on page 123](#)
- [Allow MAC Cache for Management Traffic on page 124](#)
- [Allow Unknown MAC Flooding on page 124](#)
- [Skip TCP Sequence Number Check on page 124](#)

- [TCP RST Invalid Session on page 124](#)
- [Check TCP SYN Bit Before Create Session on page 125](#)
- [Check TCP SYN Bit Before Create Session for Tunneled Packets on page 125](#)
- [Use SYN-Cookie for SYN Flood Protection on page 125](#)
- [Enforce TCP Sequence Number Check on TCP RST Packet on page 126](#)
- [Use Hub-and-Spoke Policies for Untrust MIP Traffic on page 126](#)
- [Max Fragmented Packet Size on page 127](#)
- [Flow Initial Session Timeout \(Seconds\) on page 127](#)
- [Multicast Flow Configuration on page 127](#)
- [TCP MSS on page 127](#)
- [All TCP MSS on page 127](#)
- [GRE In TCP MSS on page 128](#)
- [GRE Out TCP MSS on page 128](#)
- [Aging on page 128](#)

## ICMP Path MTU Discovery

The ICMP Path MTU Discovery option controls how the security device handles a packet that meets the following conditions: the Don't Fragment (DF) bit is set in the IP header, the packet is intended for IPsec encapsulation, and the size of the packet after encapsulation exceeds the maximum transfer unit (MTU) of the egress interface, which is 1500 bytes:

- When this option is enabled, the security device sends the source host an ICMP message indicating the packet size is too large (ICMP type 3, code 4 "Fragmentation needed and DF set" ).
- When this option is disabled, the security device ignores the DF bit, encapsulates the packet, fragments the packet so that none of the fragmented packets exceeds the MTU of the egress interface, and forwards them through the appropriate VPN tunnel.

By default, this option is disabled.

## Allow DNS Reply Without Matched Request

Use the Allow DNS Reply Without Matched Request option to control how the security device handles DNS reply packets that do not have a matching DNS request:

- When this option is enabled, the security device does not verify that a DNS reply packet has a matching request.
- When this option is disabled and the security device receives an incoming UDP first-packet that has a destination port of 53, the device checks the DNS message packet header to verify that the query (QR) bit is 0 (0 = query message). If the QR bit is 1 (1 = response message) the device drops the packet, does not create a session, and increments the illegal packet flow counter for the receiving interface.

By default, this option is disabled.

## Allow MAC Cache for Management Traffic

Use the Allow Mac Cache for Management Traffic option to control how the security device handles a source MAC address for administrative traffic:

- When this option is enabled, the security device caches the source MAC address from incoming administrative traffic, and then uses that address when replying. You might need to enable this option for managed devices that use source-based routing.
- When disabled, the security device does not cache the source MAC address from incoming administrative traffic.

By default, this option is disabled.

## Allow Unknown MAC Flooding

Use the Allow Unknown MAC Flooding option to control how the security device handles a packet that has a destination MAC address that is not in the MAC learning table:

- When this option is enabled, the security device permits the packet to cross the firewall.
- When this option is disabled, the security device drops the packet and does not permit it to cross the firewall.

By default, this option is enabled.

## Skip TCP Sequence Number Check

Use the Skip TCP Sequence Number Check to control how the security device handles TCP packets with an out-of-sequence TCP number:

- When this option is enabled, the security device does not monitor the TCP sequence number in TCP segments during stateful inspection.
- When this option is disabled, the security device detects the window scale specified by both hosts in a session and adjusts a window for an acceptable range of sequence numbers according to their specified parameters. The device monitors the sequence numbers in packets sent between these hosts; if the device detects a sequence number outside this range, it drops the packet.

By default, this option is enabled.

## TCP RST Invalid Session

Use the TCP RST Invalid Session to control how the security device handles a TCP reset packet (a TCP packet with the RST flag set):

- When this option is enabled and the security device receives a TCP reset packet, the device marks the session for immediate termination.
- When this option is disabled, the security device marks the session to termination after the normal session timeout interval. Normal session timeout intervals for common protocols:
  - The TCP session timeout is 30 minutes.



- The UDP session timeout is 1 minute.
- The HTTP session timeout is 5 minutes.

By default, this option is disabled.

### Check TCP SYN Bit Before Create Session

Use the TCP SYN Bit Before Create Session option to control how the security device handles a set SYN bit in the first packet of a session:

- When this option is enabled, the security device checks that the SYN bit is set in the first packet of a session. If the SYN bit is not set, the device drops the packet and does not create the session.
- When this option is disabled, the security device does not enforce SYN checking before creating a session.

By default, security devices running ScreenOS 5.1 and later have this option enabled. However, in previous versions of ScreenOS, this option was disabled. If you upgraded from a ScreenOS release prior to ScreenOS 5.1 and did not change the default setting for this option, SYN checking remains disabled.

The security devices running ScreenOS 6.3 send a TCP session close notification acknowledgement (ACK) to both the client and the server when a session is being closed. To enable a policy to send a TCP session close notification, complete the following prerequisites:

- Enable the TCP SYN checking and the TCP reset options in both the client and the server zones.
- Enable the TCP sequence check only for ISG1000 or ISG2000 and NetScreen-5200 or NetScreen-5400.

### Check TCP SYN Bit Before Create Session for Tunneled Packets

Use the TCP SYN Bit Before Create Session for Tunneled Packets option to control how the security device handles a set SYN bit in the first packet of a VPN session:

- When this option is enabled, the security device checks that the SYN bit is set in the first packet arriving in a VPN tunnel. If the SYN bit is not set, the device drops the packet and does not create the session.
- When this option is disabled, the security device does not enforce SYN checking before creating a session in a VPN tunnel.

By default, this option is enabled.

### Use SYN-Cookie for SYN Flood Protection

Use the SYN-Cookie for SYN Flood Protection option as an alternative to traditional SYN proxying mechanisms to help reduce CPU and memory usage:

- When this option is enabled on the security device, SYN-cookie becomes the TCP-negotiating proxy for the destination server, and replies to each incoming SYN segment with a SYN/ACK containing an encrypted cookie as its initial sequence number (ISN). The cookie is a MD5 hash of the original source address and port number, destination address and port number, and ISN from the original SYN packet. After sending the cookie, the security device drops the original SYN packet and deletes the calculated cookie from memory.
- When this option is disabled, traditional SYN-proxy becomes the TCP-negotiating proxy for the destination server.

By default, this option is disabled.



**NOTE:** This option is only available on devices running ScreenOS 5.2 and later.

---

## Enforce TCP Sequence Number Check on TCP RST Packet

Use the Check TCP Sequence Number Check on TCP RST Packet option to control how the security device handles TCP reset (RST) packets with an out-of-sequence TCP number:

- When this option is enabled, the security device monitors the TCP sequence number in a TCP segment with the RST bit enabled. If the sequence number matches the previous sequence number for a packet in that session or is the next higher number incrementally, the device permits the packet to cross the firewall. If the sequence number does not match either of these expected numbers, the device drops the packet and sends the host a TCP ACK segment with the correct sequence number.
- When this option is disabled, the security device does not monitor the TCP sequence number in TCP segments that have an RST bit enabled.

By default, this option is disabled.



**NOTE:** The NetScreen 5000 line does not support this option.

---

## Use Hub-and-Spoke Policies for Untrust MIP Traffic

Use this option to control how the security device handles the forwarding of packets arriving in a VPN tunnel to and from a mapped IP (MIP) address:

- When this option is enabled, the security device forwards traffic arriving through a VPN tunnel to a MIP address on one tunnel interface to the MIP host at the end of another VPN tunnel. The two tunnels form a hub-and-spoke configuration, with the traffic looping back on the same outgoing interface.
- When this option is disabled, the security device does not forward VPN traffic arriving at a MIP to a MIP at the other end of the VPN tunnel.

By default, this option is enabled.



**NOTE:** This option affects traffic forwarding only when the outgoing interface is bound to the Untrust zone.

## Max Fragmented Packet Size

Use the Max Fragmented Packet Size option to control the maximum size of a packet fragment generated by the security device. You can set the number value between 1024 and 1500 bytes inclusive. For example, if a received packet is 1500 bytes and this option is set to 1460 bytes, the device generates two fragment packets: The first is 1460 bytes and the second is 40 bytes. If you reset this option to 1024, the first fragment packet is 1024 bytes and the second is 476 bytes.

By default, this option is set to none.

## Flow Initial Session Timeout (Seconds)

Use the Flow Initial Session Timeout to control the number of seconds the security device keeps an initial TCP session in the session table before dropping it or receiving a FIN or RST packet. You can set the number of seconds from 20 seconds to 300 seconds.

By default, this option is set to 20 seconds.

## Multicast Flow Configuration

In earlier versions, all TCP, UDP, and ICMP traffic was supported by setting policy rules. Use this option to inspect IDP multicast traffic for devices running ScreenOS 6.3.

## TCP MSS

Use the TCP MSS option to control how the security device handles the TCP-MSS value for TCP SYN packets in an IPsec VPN tunnel:

- When this option is set to Packet Size, the security device modifies the MSS value in a TCP packet to avoid fragmentation caused by the IPsec operation. The default MSS for this option is 1400.
- When this option is disabled, the security device does not modify the MSS value in a TCP packet.

By default, this option is disabled.



**NOTE:** When you configure a value for the All TCP MSS option, that value overrides the settings defined for this option.

## All TCP MSS

Use the All TCP-MSS to control how the security device handles the TCP MSS value for TCP SYN packets in all network traffic:

- When this option is set to Packet Size, the security device modifies the MSS value in a TCP packet to avoid fragmentation by other network components. You can set the TCP MSS range from 0 to 65,535 bytes; the default MSS for this option is set to none.

Additionally, this option overrides the configuration for TCP MSS (described earlier):

- If the TCP MSS option for IPsec VPN traffic is not set, the security device applies the value specified in this option for TCP packets in an IPsec VPN tunnel.
  - If the TCP MSS option for IPsec VPN traffic is set, the security device overrides that value with the value from the All TCP MSS option.
- When this option is disabled, the security device does not modify the MSS value of a TCP packet in network traffic.

By default, this option is disabled.

## GRE In TCP MSS

Use the GRE in TCP MSS option to control how the security device handles the TCP MSS value for generic routing encapsulation (GRE) packets destined for an IPsec VPN tunnel.

- When this option is set to Packet Size, the security device modifies the MSS value in a GRE packet to avoid fragmentation caused by the IPsec operation. The TCP MSS range is 64 to 1420 bytes inclusive; the default MSS for this option is 1320.
- When this option is disabled, the security device does not modify the MSS value in a GRE packet entering an IPsec VPN tunnel.

By default, this option is disabled.

## GRE Out TCP MSS

Use the GRE Out TCP MSS option to control how the security device handles the TCP MSS value for GRE packets leaving an IPsec VPN tunnel.

- When this option is set to Packet Size, the security device modifies the MSS value in a GRE packet to avoid fragmentation caused by the IPsec operation. The TCP MSS range is 64 to 1420 bytes inclusive; the default MSS for this option is 1320.
- When this option is disabled, the security device does not modify the MSS value in a GRE packet leaving an IPsec VPN tunnel.

By default, this option is disabled.

## Aging

Use the Aging options to control how the security device uses aggressive aging to affect session timeout. Aggressive aging begins when the number of entries in the session table exceeds the high-watermark setting, and ends when the number of sessions falls below the low-watermark setting. When aggressive aging is in effect, the security device ages out sessions—beginning with the oldest sessions first—at the rate you specify.

When the session table is in any other state, the normal session timeout value is applied. Normal session timeout intervals for common protocols:

- The TCP session timeout is 30 minutes.
- The UDP session timeout is 1 minute.
- The HTTP session timeout is 5 minutes.

### Early Ageout Time Before the Session's Normal Ageout

Use this aging option to control how the security device uses aggressive aging to age out a session from its session table. The value range is 2 to 10 units, where each unit is 10 seconds; by default, the early-ageout value is 2 or 20 seconds.

### Percentage of Used Sessions Before Early Aging Begins

Use this aging option to control when the security device begins aggressive aging. The value range is 1 to 100, which indicates percent of the session table capacity. By default, this option is set to 100% (used sessions must account for 100% of the session table capacity before aggressive aging begins).

### Percentage of Used Sessions Before Early Aging Stops

Use this aging option to control when the security device ends aggressive aging. The value range is 1 to 100, which indicates percent of the session table capacity. By default, this option is set to 100% (used sessions must account for 100% of the session table capacity before aggressive aging ends).

#### Related Documentation

- [Allocating Network Bandwidth Using Traffic Shaping Options on page 119](#)
- [Configuring Features Unsupported in NSM Using Supplemental CLI Options Overview on page 129](#)
- [Enabling/Disabling Application Layer Gateway Protocols Overview on page 121](#)

## Configuring Features Unsupported in NSM Using Supplemental CLI Options Overview

Use the supplemental CLI option to configure features on security devices not yet formally supported in NSM. This applies to security devices running a future release of ScreenOS.



**NOTE:** We recommend that you use the Supplemental CLI to configure features in future versions of ScreenOS only. When you perform an update, the CLI commands that you specify are sent unconditionally to the security device. NSM does not validate whether or not these commands are sent successfully. Validation errors may occur if you edit the actual configuration on the device using the supplemental CLI.

#### Related Documentation

- [Configuring ScreenOS with TFTP or FTP Servers Enabled Using TFTP/FTP Options on page 130](#)
- [Configuring Hostnames and Domain Names Overview on page 130](#)
- [Using Packet Flow Options on page 122](#)

## Configuring ScreenOS with TFTP or FTP Servers Enabled Using TFTP/FTP Options

---

Use the TFTP/FTP option to configure a security device running to enable TFTP or FTP servers to save or import external files. These external files include configuration files (.cfg), ScreenOS firmware versions, public keys, error messages, certificates, and other items.

For security devices running ScreenOS 5.0 or later, NSM does not use the TFTP server on the security device to download ScreenOS firmware versions, certificates, and CRLs to the managed device. To perform these tasks, you must install a TFTP server on the NSM device server. For details, see the *Network and Security Manager Installation Guide*.



**NOTE:** For security devices running ScreenOS 5.1 and later, Network Security Manager uses SSP to download ScreenOS firmware versions, certificates, and CRLs to the managed device.

For TFTP servers, you can specify the following options:

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

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

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

### Related Documentation

- [Configuring Hostnames and Domain Names Overview on page 130](#)
- [Configuring Features Unsupported in NSM Using Supplemental CLI Options Overview on page 129](#)
- [Configuring NSGP Overview on page 131](#)

## Configuring Hostnames and Domain Names Overview

---

The Host/Domain Name option enables you to configure a host and domain name for the security device. The host name is a character string that identifies the device. The host name, combined with a domain name, enables other devices to access the security device through a DNS server. If you define a fully qualified domain name (FQDN) for the device, you can use the FQDN as a gateway for a VPN tunnel.

For information about how to configure a hostname or domain name for a security device, see the **hostname** and **domain** commands in the *NetScreen CLI Reference Guide*.

- Related Documentation**
- [Configuring NSGP Overview on page 131](#)
  - [Configuring ScreenOS with TFTP or FTP Servers Enabled Using TFTP/FTP Options on page 130](#)
  - [NSGP Modules Overview on page 131](#)

## Configuring NSGP Overview

NetScreen Gatekeeper Protocol (NSGP) is a Juniper Networks proprietary peer-to-peer protocol that enables a security device to act as a server for voice-over-IP (VoIP) traffic:

- NetScreen-500 security devices running ScreenOS 5.0 GPRS can be both the NSGP server and client.
- NetScreen-500 and NetScreen 5000 line security devices running ScreenOS 5.0 NSGP or 5.1 and later can only be an NSGP server.



**NOTE:** To use NSGP on a NetScreen-500 or NetScreen 5000 line device, you must first enable NSGP using a license key. For information about activating NSGP using a license key, see the *Network and Security Administration Guide*.

You can use NSGP to prevent overbilling attacks that can occur when using the GPRS tunneling protocol (GTP) for VoIP. By configuring one security device as an NSGP server and another security device as a GTP client, you can keep both server and client aware of the connection status. When a user initiates a call, the NSGP server and GTP client establish a session; when the user completes the call, the client notifies the server, prompting the server to close the session.

Configuring NSGP on a device *does not* automatically enable the device to handle GTP traffic—it enables the GTP client and NSGP server to close a session at the same time. To enable the GTP client to manage GPRS traffic, you must create a GTP object, and then add that object to the security policy installed on the device. For details on creating a GTP object and adding a GTP object to a security policy, see the *Network and Security Manager Administration Guide*.

- Related Documentation**
- [NSGP Modules Overview on page 131](#)
  - [Configuring Hostnames and Domain Names Overview on page 130](#)
  - [Example: Configuring NSGP on GTP and Gi Firewalls \(NSM Procedure\) on page 132](#)

## NSGP Modules Overview

Because each mobile station (MS) gets an IP address from an IP pool, an overbilling attack can occur when a legitimate subscriber returns an IP address to the IP pool, but the session is still open. Attackers can hijack the open session without being detected and reported, then download data at the expense of the legitimate subscriber, or send

data to other subscribers. Overbilling can also occur when a newly returned IP address is reassigned to another MS; traffic initiated by the previous MS might be forwarded to the new MS, causing the new MS to be billed for unsolicited traffic. To protect subscribers of a public land mobile network (PLMN) from overbilling attacks, you can use the NetScreen Gatekeeper Protocol (NSGP) module and two security devices.

The NSGP module includes two components: the client and the server. The client connects to the server and sends requests, which the server processes. Both client and server support multiple connections to each other and to others simultaneously. Using TCP, NSGP monitors the connectivity between client and server by sending Hello messages at set intervals.

NSGP uses a session context to ensure that the server and client know that status of the connection. The session context stores is identified by a unique number (context ID); when configuring NSGP on the client and server devices, you must use the same context ID on each device. When the client sends a “clear session” request to the server, the request includes the context ID and IP address of the server. When the server receives the “clear session” message, it matches the context ID and then clears the session from its table.

The security device acting as the NSGP server must run the ScreenOS 5.0 GPRS firmware, and the other device acting as the GTP client must run the ScreenOS 5.0 NSGP firmware. After you have deployed the two devices, you must:

- Configure NSGP on the GTP server to recognize when a GTP tunnel is deleted and to notify the GTP client.
- Configure NSGP on the GTP client to automatically clear sessions whenever the NSGP server gets a notification from the GTP client that a GTP tunnel was deleted.

By clearing the sessions, the NSGP server stops the unsolicited traffic and prevents overbilling.

**Related  
Documentation**

- [Configuring NSGP Overview on page 131](#)
- [Configuring Hostnames and Domain Names Overview on page 130](#)
- [Example: Configuring NSGP on GTP and Gi Firewalls \(NSM Procedure\) on page 132](#)

---

## Example: Configuring NSGP on GTP and Gi Firewalls (NSM Procedure)

In this example, you configure NSGP on both the GTP firewall (client) and the Gi firewall (server). First, you must create the GTP object for the client connection. Then, to enable NSGP on the security device, you must configure both the server and client side connection parameters:

- For the NSGP server connection, you enable NSGP on an interface.
- For the GTP client connection, you select a source interface, and then copy the NSGP server settings (from the NSGP server device) to configure the destination interface.



Finally, you create a firewall rule that includes the GTP object, the GTP firewall, and the Gi firewall.

To configure a firewall rule:

1. Create a GTP object named GPRS1. For information about how to create a GTP object, see the *Network and Security Manager Administration Guide*.
2. Add the Gi Firewall (server) as a NetScreen-500 running ScreenOS 5.1, and then configure the network module:
  - Double-click the device icon to open the device configuration. In the device navigation tree, select **Network > Slot**.
  - Double-click slot 1 to display the slot configuration dialog box. For Card Type, select **2 Interfaces (10/100)**, and then click **OK**.
3. Add the GTP firewall (client) as a NetScreen-500 running ScreenOS 5.0 GPRS, and then configure the network module:
  - Double-click the device icon to open the device configuration. In the device navigation tree, select **Network > Slot**.
  - Double-click slot 1 to display the slot configuration dialog box. For Card Type, select **2 Interfaces (10/100)**.
  - Click **OK** to save the slot configuration.
4. Configure the Gi firewall (server):
  - In the device navigation tree, select **Advanced > NSGP Server Side**.
  - Leave the default port number and enter an MD5 password.
5. In the NSGP Context IDs area, click the **Add** icon to display the New Context Entry dialog box. Configure the following options, and then click **OK**:
  - For Context Entry, enter **2**.
  - For Zone, select **untrust**.
6. In the Interface NSGP Settings area, right-click **ethernet1/2** and select **Edit** icon. The General Properties screen appears. Configure the following options:
  - Ensure that the Zone is untrust and the Mode is Route.
  - For IP Address, enter **2.2.1.4**.
  - For Netmask, enter **24**.
  - Ensure that Manageable is enabled and that the Management IP is 2.2.1.4.
7. In the interface navigation tree, select **Service Options**. Configure the following options:
  - Select **Telnet**.
  - Select **NSGP Enabled**.
  - Select **Enforce IPSec** to encrypt the GTP connection.

8. Click **OK** to save your changes to the interface, and then click **OK** to save your changes to the device.
9. Configure the GTP firewall (client):
  - In the device navigation tree, select **Advanced > NSGP > NSGP Connections**. Click the **Add** icon to display the New NSGP Connection dialog box.
  - For Source Interface, select **ethernet 1/2**.
  - For Destination, click **Copy Existing NSGP Server Setting**. The Copy Existing NSGP Server Info dialog box appears.
10. Configure the following:
  - For NSGP Server Info, select **Gi firewall** (server).
  - For Destination Interface, select **ethernet1/2**.
11. Click **OK** to copy the NSGP server settings to the GTP client. NSM automatically completes the destination server settings for the GTP client.
12. In GTP Objects, select the GPRS1 object.
13. Click **OK** to save the NSGP Connection.
14. Configure a firewall rule to handle GTP traffic.

**Related  
Documentation**

- [Configuring Hostnames and Domain Names Overview on page 130](#)
- [Configuring NSGP Overview on page 131](#)
- [Using the PPP Option to Configure Point-To-Point Protocol Connections on page 134](#)

---

## Using the PPP Option to Configure Point-To-Point Protocol Connections

Use the PPP option to configure how the device handles Point-to-Point Protocol (PPP) connections. PPP encapsulation allows different Network Layer protocols to be multiplexed simultaneously over commonly used physical links. To establish a PPP connection, you configure each end of a PPP link by exchanging Link Control Protocol (LCP) packets. LCP is used to establish, configure, and test data-link options. These options include encapsulation format options, authentication of the peer on the link, handling of varying limits on sizes of packets, detecting a looped-back link and other common misconfiguration errors; determining when a link is functioning properly or failing; and terminating the link.

PPP allows for authentication during link establishment to permit or deny connection to a device. This authentication can be performed using either Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP). These authentication protocols are intended for use primarily by hosts and routers that connect to a network server through switched circuits or dial-up lines but can also be used with dedicated lines.

For an interface with PPP encapsulation, you must configure a PPP access profile and bind it to the interface. You create an access profile with a user-defined name that is

unique on the SSG device. You can bind the same access profile to more than one interface, but only one profile can be assigned to an interface. A PPP access profile includes the following information:

- PPP profile name
- Auth local name
- Auth secret
- Auth type
- Passive mode chap
- Static IP
- Netmask

**Related  
Documentation**

- [About Configuring PPPoE on page 135](#)
- [Example: Configuring NSGP on GTP and Gi Firewalls \(NSM Procedure\) on page 132](#)
- [Using the PPP Option to Configure Point-To-Point Protocol Connections on page 134](#)

## About Configuring PPPoE

Use the PPPoE option to configure how the device handles Point-to-Point Protocol over Ethernet (PPPoE) connections. PPPoE enables multiple users at a site to share the same digital subscriber line, cable modem, or wireless connection to the Internet. Some security devices support PPPoE, which enables them to operate compatibly on DSL, Ethernet Direct, and cable networks run by ISPs that use PPPoE for their clients' Internet access.



**NOTE:** Some ISPs use DHCP for their clients' Internet access. To configure DHCP on an interface, see [“Example: Assigning TCP/IP Settings for Hosts Using DHCP \(NSM Procedure\)” on page 58](#). For more detailed explanation about PPPoE or DHCP on security devices, see the “Fundamentals” volume in the *Concepts & Examples ScreenOS Reference Guide*.

On devices that support PPPoE, you can configure a PPPoE client instance on any or all interfaces. You configure a specific instance of PPPoE with a username and password and other parameters, and bind the instance to an interface. When two Ethernet interfaces (a primary and a backup) are bound to the Untrust zone, you can configure one or both interfaces for PPPoE. Specifically:

- For all security devices running ScreenOS 5.0 and later, you can enable PPPoE on multiple interfaces in any zone at the same time.
- For all security devices running ScreenOS 5.1 and later, you can bind a PPPoE instance to a:
  - VSI interface—Use this option when running two devices using NSRP in active-passive mode. When failover occurs, the new primary device can use the same IP as the

previous primary device to continue communicating with the ISP. Because the PPPoE connection is maintained, downtime during failover is minimized. To bind PPPoE instance to a VSI interface, you must have already created the NSRP cluster and the VSI interfaces.

- Subinterface—Use this option to enable multiple PPPoE sessions on one physical interface. To bind the PPPoE instance to a subinterface, you must have already created the subinterface. For details, see [“Example: Configuring a Subinterface \(NSM Procedure\)” on page 84.](#)



**NOTE:** The number of PPPoE sessions per physical interface is determined by the security device platform.

#### Related Documentation

- [Example: Updating DNS Servers \(NSM Procedure\) on page 136](#)
- [Example: Configuring NSGP on GTP and Gi Firewalls \(NSM Procedure\) on page 132](#)
- [Using the PPP Option to Configure Point-To-Point Protocol Connections on page 134](#)

### Example: Updating DNS Servers (NSM Procedure)

When you initiate a PPPoE connection, your ISP automatically provides the IP addresses for the Untrust zone interface and the IP addresses for the Domain Name System (DNS) servers. When the device receives DNS addresses through PPPoE, the new DNS settings overwrite the local settings by default.

If you do not want the new DNS settings to replace the local settings, enable the Manual IP Configuration setting when configuring a PPPoE instance. If you use a static IP address for the Untrust zone interface, you must obtain the IP addresses of the DNS servers and manually enter them on the security device and on the hosts in the Trust zone.

In this example, the security device receives a dynamically assigned IP address for its Untrust zone interface (ethernet3) from the ISP. Because the device also dynamically assigns IP addresses for the three hosts in its Trust zone, the device acts both as a PPPoE client and a DHCP server. The Trust zone interface must be in either NAT mode or Route mode. In this example, it is in NAT mode.

Before setting up the site in this example for PPPoE service, you must have the following: a digital subscriber line (DSL) modem and line, an account with an ISP, and a username and password (obtained from the ISP).

To update a DNS server:

1. Add a NetScreen-5GT device running ScreenOS 5.0 named “Device A.”
2. Configure the ethernet1 interface (Trust Interface):
  - In the device navigation tree, select **Network > Interface**.
  - Double-click the **ethernet1** interface. The General Properties screen appears.

3. Configure the General Properties options:
  - For Zone, select **Trust** (default setting).
  - For IP Address, enter **172.16.30.10**.
  - For Netmask, enter **24**.
  - Ensure that Manageable is enabled and that the Management IP is 172.16.30.10.
  - For Interface Mode, select **NAT** (default setting).
4. In the interface navigation tree, select **DHCP**. Set the DHCP mode to **DHCP Server** and configure as follows:
  - For DNS #1, DNS #2, and Client Gateway, enter **0.0.0.0**.
  - For Lease Time, enter **60** (60 minutes).
  - Leave all other defaults.
5. Select the **IP Pools** tab, and then click the **Add** icon. the New DHCP IP Pool dialog box appears. Configure the following:
  - For IP Address, enter **172.16.30.2**.
  - For Value, select **End IP**.
  - For End of Dynamic IP Range, enter **172.16.30.5**.
6. Click **OK** to save the new IP Pool, and then click **OK** to save your changes to the interface.
7. Configure the ethernet3 interface (Untrust Interface):
  - In the device navigation tree, select **Network > PPPoE**.
8. Click the **Add** icon. The New PPPoE Instance dialog box appears. Configure the following options:
  - For PPPoE Instance, enter **eth3-pppoe**.
  - For Interface, select **ethernet3**.
  - For username, enter **user1**.
  - For password, enter **123456**.
  - For Concentrator-Name, enter **ac-11**.
  - Leave all other defaults.
9. Click **OK** to add the instance, and then click **OK** again to save your changes to the device.
10. Activate PPPoE and DHCP on the network.
11. Turn off the power to the DSL modem, the security device, and any connected workstations.
12. Turn on the DSL modem.

13. Turn on the security device. The device makes a PPPoE connection to the ISP and, through the ISP, gets the IP addresses for the DNS servers.
14. Activate DHCP on the internal network, by turning on the workstations. The workstations automatically receive the IP addresses for the DNS servers. They get an IP address for themselves when they attempt a TCP/IP connection. Every TCP/IP connection that a host in the Trust zone makes to the Untrust zone automatically goes through the PPPoE encapsulation process.

**Related Documentation**

- [Example: Configuring Multiple PPPoE Sessions on a Single Interface \(NSM Procedure\) on page 138](#)
- [About Configuring PPPoE on page 135](#)
- [Configuring a PPPoA Client Instance on page 141](#)

## **Example: Configuring Multiple PPPoE Sessions on a Single Interface (NSM Procedure)**

Some security devices support multiple PPPoE subinterfaces (each with the same MAC address) for a given physical interface. On such devices, you can make a PPPoE connection on multiple instances by binding each subinterface to a different PPPoE instance. You can determine which traffic the device sends over a particular PPPoE session by configuring routes that specify a specific PPPoE sub-interface for each session (no rules determine the flow of traffic). IPsec tunnels can terminate on such PPPoE subinterfaces.

The maximum number of concurrent PPPoE sessions on a physical interface is limited only by the number of subinterfaces allowed by the device. There is no restriction on how many physical interfaces can support multiple sessions. You can specify username, static-ip, idle-timeout, auto-connect and other parameters separately for each PPPoE instance or session.

To support a PPPoE session, a subinterface must be untagged. A tagged sub-interface uses an associated VLAN tag to enable the subinterface to receive Layer 2 traffic and direct it selectively to a particular VLAN, which usually resides in a trusted zone. VLAN tags allow a single physical interface to direct exchanged packets selectively to and from VLANs, each through a different subinterface.

By contrast, an untagged interface does not use a VLAN tag to identify a VLAN for an subinterface. Instead, it uses a feature called encap, which binds the subinterface to a particular defined PPPoE definition. By hosting multiple subinterfaces, a single physical interface can host multiple PPPoE instances. You can configure each instance to go to a specified AC (access concentrator), thus enabling separate entities (such as ISPs) to manage the PPPoE sessions through a single interface.

In the following example you define three PPPoE instances:

- Instance `isp_new_york`, password "swordfish," bound to interface `ethernet3`. This instance provides access to a service named `Big_Apple_Service`. The AC is named `isp_ny_ac`.

- Instance `isp_los_angeles`, password “ marlin,” bound to subinterface `ethernet3.1`. This instance provides access to a service named `Angels_Service` . The AC is named `isp_la_ac` .
- Instance `isp_chicago`, password “ trout,” bound to subinterface `ethernet3.2`. This instance provides access to a service named `Windy_City_Service` . The AC is named `isp_c_ac` .

To configure multiple PPPoE sessions on a single interface:

1. Add a NetScreen-208 device running ScreenOS 5.1 named “Device A” .
2. In the NSM navigation tree, select **Devices > Security Devices**. Double-click Device A to open the device configuration.
3. In the device navigation tree, select **Network > Interfaces**. Configure the subinterfaces for the Los Angeles and Chicago ISPs.

Click the **Add** icon and select **Sub Interface**. The General Properties screen appears. Configure the following options:

- For Name, select **ethernet 3**.
  - For Tag, select **1**.
  - For Sub Interface Type, select **encap**.
  - For Encap, select **pppoe**.
  - For Zone, select **Untrust**.
4. Leave all other defaults and click **OK** to save the new subinterface.
  5. Click the **Add** icon and select **Sub Interface**. The General Properties screen appears. Configure as follows:
    - For Name, select **ethernet 3**.
    - For Tag, select **2**.
    - For Sub Interface Type, select **encap**.
    - For Encap, select **pppoe**.
    - For Zone, select **Untrust**.
    - Leave all other defaults and click **OK** to save the new subinterface.
  6. Configure the PPPoE Instance for the New York ISP:
    - In the device navigation tree, select **Network > PPPoE**.
    - Click the **Add** icon. The New PPPoE Instance dialog box appears.
  7. Configure the following options, and then click **OK**:
    - For Name, enter **isp\_new\_york**.
    - For Interface, select the physical interface **ethernet3**.
    - For Username, enter **user1@domain1**.
    - For Password, enter **swordfish**.

- For Access Concentrator, enter **isp\_ny\_ac**.
  - For Service, enter **Big\_Apple\_Service**.
  - Select **Clear On Disconnect**.
  - Leave all other defaults.
8. Configure the PPPoE Instance for the Los Angeles ISP:
- In the device navigation tree, select **Network > PPPoE**.
  - Click the **Add** icon. The New PPPoE Instance dialog box appears.
9. Configure the following options, and then click **OK**:
- For Name, enter **isp\_los\_angeles**.
  - For Interface, select the subinterface **ethernet3.1**.
  - For Username, enter **user2@domain2**.
  - For Password, enter **marlin**.
  - For Access Concentrator, enter **isp\_la\_ac**.
  - For Service, enter **Angels\_Service**.
  - Select **Clear On Disconnect**.
  - Leave all other defaults.
10. Configure the PPPoE Instance for the Chicago ISP:
- In the device navigation tree, select **Network > PPPoE**.
  - Click the **Add** icon. The New PPPoE Instance dialog box appears.
11. Configure the following options, and then click **OK**:
- For Name, enter **isp\_chicago**.
  - For Interface, select the subinterface **ethernet3.2**.
  - For Username, enter **user3@domain3**.
  - For Password, enter **trout**.
  - For Access Concentrator, enter **isp\_c\_ac**.
  - For Service, enter **Windy\_City\_Service**.
  - Select **Clear On Disconnect**.
  - Leave all other defaults.
12. Click **OK** to save your changes to the device.

**Related Documentation**

- [Configuring a NetScreen Address Change Notification on page 141](#)
- [Example: Updating DNS Servers \(NSM Procedure\) on page 136](#)
- [Configuring a PPPoA Client Instance on page 141](#)



## Configuring a PPPoA Client Instance

PPPoA is typically used for PPP sessions that terminate on a security device with an ADSL interface (the NetScreen-5GT ADSL security device). On the ADSL interface (or its subinterfaces), you can configure a PPPoA client instance with a username, password, and other parameters, and then bind the instance to the ADSL interface (or subinterface).

When the NetScreen-5GT ADSL security device initiates a PPPoA connection to the PPPoA server (controlled by the service provider), the server automatically provides the IP addresses for the Untrust zone interface and for the Domain Name System (DNS) servers. Using this information, the security device automatically updates the DNS server addresses in its DHCP server (you can disable this automatic update if desired).

For details and an example of configuring an ADSL interface with PPPoA, see [“ADSL Interface in ScreenOS Devices” on page 88](#).

### Related Documentation

- [Example: Configuring Multiple PPPoE Sessions on a Single Interface \(NSM Procedure\) on page 138](#)
- [Configuring a NetScreen Address Change Notification on page 141](#)
- [Interface Failover in ScreenOS Devices on page 141](#)

## Configuring a NetScreen Address Change Notification

Use the NACN option to configure NetScreen Address Change Notification (NACN). NACN is available only on security devices running ScreenOS 5.0.x. Before NSM can contact a security device, it must have the current IP address of the device interface. This is relatively easy when the security device has a static IP address on its interface. However, an interface on a security device can have a dynamically assigned IP address, using either PPPoE or DHCP. In these cases, the security device uses NACN to monitor a specific interface and then register with NSM the IP address of the interface whenever it changes. This prevents interruption of communication between NSM and the security device.

For more detailed explanation about NACN on security devices, see the “Administration” volume in the *Concepts & Examples ScreenOS Reference Guide* for ScreenOS 5.0.0.

### Related Documentation

- [Configuring a PPPoA Client Instance on page 141](#)
- [Example: Configuring Modem Connections \(NSM Procedure\) on page 142](#)
- [Interface Failover in ScreenOS Devices on page 141](#)

## Interface Failover in ScreenOS Devices

The Failover is only available for some security devices. Use the Failover option to configure the security device to switch over traffic from the primary interface to the backup interface, and from the backup to the primary when there are both primary and backup interfaces bound to the Untrust zone. An interface failover can occur when ScreenOS detects a

physical link problem on the primary interface connection, such as an unplugged cable. You can also define the following types of interface failover:

- When certain IP addresses become unreachable through a given interface using IP tracking
- When certain VPN tunnels on the primary untrust interface become unreachable using VPN tunnel monitoring

You can also configure the security device to automatically switch to the backup interface if ScreenOS detects a failure on the primary interface connection. When the connection through the primary interface is restored, ScreenOS automatically switches traffic from the backup interface to the primary.

By default, there is a 30-second interval before the failover occurs (the hold-down time). You can change this interval.

For more detailed explanation about interface failover on security devices, see the “High Availability” volume in the *Concepts & Examples ScreenOS Reference Guide*.

#### Related Documentation

- [Configuring a PPPoA Client Instance on page 141](#)
- [Example: Configuring Modem Connections \(NSM Procedure\) on page 142](#)
- [Example: Creating Modem Settings \(NSM Procedure\) on page 143](#)

## Example: Configuring Modem Connections (NSM Procedure)

The modem is only available for some security devices. Use the Modem option to configure the security device for operation with an external modem. You can connect an external modem to the RS-232 serial port on certain security devices to enable the device to establish a PPP connection to an ISP. This provides a backup serial interface for traffic to the Untrust zone if there is a failure on the connection through the primary interface.

You can configure the parameters for the serial link as described in [Table 30 on page 142](#).

**Table 30: Parameters for Serial Link**

Parameters	Range Value
Speed (BPS)	The maximum baud rate for the serial link (the default rate is 115,200 bps).
Timeout	The maximum amount of time that the serial link can be idle before ScreenOS automatically disconnects the modem (the default is 10 minutes).
Retry Number	The number of times ScreenOS retries the dial-up connection if the line is busy or there is no response (the default is 3 times).
Retry Interval	The interval, in seconds, between dial-up retries (the default is 10 seconds).

#### Related Documentation

- [Example: Creating Modem Settings \(NSM Procedure\) on page 143](#)
- [Example: Creating ISP Connection Settings \(NSM Procedure\) on page 143](#)

- [Interface Failover in ScreenOS Devices on page 141](#)

---

## Example: Creating Modem Settings (NSM Procedure)

The modem you use for the dial-up connection must support the following features:

- Hardware flow control
- Clear-to-send (CTS) signals
- Request-to-send (RTS) signals
- Asynchronous only
- AT command set

To create the settings for a modem:

1. Click the **Add** icon in the Modem Settings portion of the Modem configuration screen.
2. Specify the name for the modem setting.
3. Specify the modem initialization string. The modem initialization string must meet the following requirements:
  - Hardware flow control is recommended, but not required (you can specify no flow control).
  - Software flow control is not used.
  - Result code must be displayed in verbal mode.
4. Specify whether this modem setting is active. You can activate only one of the configured modem settings at a time.
5. Click **OK**.

### Related Documentation

- [Example: Creating ISP Connection Settings \(NSM Procedure\) on page 143](#)
- [Setting ISP Priority for Failover on page 144](#)
- [Example: Configuring Modem Connections \(NSM Procedure\) on page 142](#)

---

## Example: Creating ISP Connection Settings (NSM Procedure)

You configure the security device to dial to an ISP account if a failover to the serial interface occurs and there is traffic to be sent. You can configure up to four ISP connections, assigning each a different priority number (1 is the highest priority). The priority number determines the order that the device uses in attempting the dial-up connection; the ISP with the highest priority is dialed first. If the device is unable to log in to the ISP account with the highest priority, it dials the ISP with the next highest priority number, and so on, until there are no more ISP configurations.

To create the settings for an ISP connection:

1. Click the **Add** icon in the ISP Settings area of the Modem configuration screen.
2. Specify the name for the ISP setting.
3. Specify the login name and password for the ISP account.



**NOTE:** All passwords handled by NSM are case-sensitive.

4. Specify the primary phone number and optionally, an alternate phone number. If the modem uses pulse dial by default but you want to use tone dial, precede the phone number with a T. If the modem uses tone dial by default but you want to use pulse dial, precede the phone number with a P.
5. Specify the priority for this setting, relative to other configured ISP settings. The highest priority is 1.
6. Click **OK**.

For more detailed explanation about interface failover on security devices, see the “High Availability” volume in the *Concepts & Examples ScreenOS Reference Guide*.

**Related  
Documentation**

- [Setting ISP Priority for Failover on page 144](#)
- [Example: Configuring Modem Connections \(NSM Procedure\) on page 142](#)
- [Example: Creating Modem Settings \(NSM Procedure\) on page 143](#)

---

## Setting ISP Priority for Failover

When using a modem connection, a trustee administrator can manually change an ISP priority. If a failover situation occurs, the priority assigned to an ISP indicates in what order relative to other ISPs that a particular ISP will be contacted. The lower the value, the higher the priority of the ISP. The trustee admin can also check the availability of an ISP with a priority setting of zero (0).

A root administrator (not a trustee admin) can configure up to four ISPs. The priority of each ISP must be a unique number. You can also configure more than one ISP with a priority of zero.

**Related  
Documentation**

- [Example: Configuring Modem Connections \(NSM Procedure\) on page 142](#)
- [Example: Creating Modem Settings \(NSM Procedure\) on page 143](#)
- [Example: Creating ISP Connection Settings \(NSM Procedure\) on page 143](#)

## CHAPTER 5

# Administration

This chapter details the administrative options for the managed device, and provides administration examples when possible. For instructions on configuring specific device settings, see the *Network and Security Manager Online Help*.

This chapter contains the following topics:

- [Device Administration Options for ScreenOS Devices Overview on page 146](#)
- [Importing Device Administrators from a Physical Device Overview on page 146](#)
- [Device Administrator Authentication Overview on page 147](#)
- [Device Administrator Account Configuration Overview on page 148](#)
- [Supporting Admin Accounts for Dialup Connections on page 151](#)
- [Restricting Management Connections Using Permitted IPs on page 152](#)
- [Local Access Configuration Using CLI Management Overview on page 153](#)
- [File Formatting in NSM Overview on page 153](#)
- [Port Numbers for SSH and Telnet Connections in NSM Overview on page 154](#)
- [Limiting Login Attempts, Setting Dial-In Authentication, and Restricting Password Length in NSM Overview on page 154](#)
- [Asset Recovery and Reset Hardware in NSM Overview on page 155](#)
- [Console-Only Connections in NSM Overview on page 156](#)
- [Secure Shell Server in NSM Overview on page 156](#)
- [Configuring CLI Banners in NSM Overview on page 158](#)
- [Configuring Remote Access Using Web Management Overview on page 159](#)
- [Configuring HTTP Administrative Connections in ScreenOS Devices Using NSM Overview on page 159](#)
- [Configuring Secure Connections in ScreenOS Devices Using NSM Overview on page 160](#)
- [Configuring Network Time Protocol and NTP Backup Server in NSM Overview on page 161](#)
- [Setting ScreenOS Authentication Options Using General Auth Settings on page 163](#)
- [Setting ScreenOS Authentication Options Using Banners Overview on page 164](#)
- [Setting ScreenOS Authentication Options Using Default Servers Overview on page 165](#)
- [Setting ScreenOS Authentication Options Using Infranet Settings Overview on page 165](#)

- [General Report Settings for ScreenOS Devices Overview on page 166](#)
- [Configuring Syslog Host Using NSM \(NSM Procedure\) on page 167](#)
- [Configuring SNMPv3 in ScreenOS Devices \(NSM Procedure\) on page 168](#)

## Device Administration Options for ScreenOS Devices Overview

---

Use the Device Administration screens to configure administrative options for the managed device. In the device navigation tree, select **Device Admin** to view configuration options.

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

### Related Documentation

- [Importing Device Administrators from a Physical Device Overview on page 146](#)
- [Device Administrator Authentication Overview on page 147](#)
- [Device Administrator Account Configuration Overview on page 148](#)

## Importing Device Administrators from a Physical Device Overview

---

A device administrator is the person responsible for managing a device locally using ScreenOS (command line or Web UI). A security device includes one default device administrator account, the root device administrator, which has complete access to all functionality on the device. Using the Network and Security Manager (NSM), you can create 20 additional device administrators with different privilege levels.



**NOTE:** To enable a device administrator to use NSM to manage devices, you must create an NSM administrator account for the device admin. For details, see *Network and Security Manager Administration Guide*.

When you import a device configuration into NSM, device administrator accounts are not automatically imported—you must manually import the accounts from the device using a separate directive. You cannot manage device administrator functionality in NSM until you have imported the device administrator information from the physical device (the device admin screens do not appear).

To notify you when device administrator information needs to be imported, NSM displays the message “Need to Migrate Admin Info From Device.” To view this message, in the device navigation tree, select **Device Administration**; the message appears in the main display area. When present, this message indicates that you have not yet imported device administrators for that device. This message automatically appears after you perform the following operations:

- Adjust the ScreenOS version—For details, see *Network and Security Administration Guide*.

To import device administrator information, from the File menu, select **Devices > Configuration > Import Admins**.



**NOTE:** The Import Admin directive lists only ScreenOS devices.

**Related  
Documentation**

- [Device Administration Options for ScreenOS Devices Overview on page 146](#)
- [Device Administrator Authentication Overview on page 147](#)
- [Device Administrator Account Configuration Overview on page 148](#)

## Device Administrator Authentication Overview

To authenticate device administrators when they attempt to connect to the security device, you can use the default authentication server (on the device) or an external authentication server.

The root device administrator is always stored and authenticated using the local database; however, for non-root read/write and read-only device admins (including vsys device admins), you can specify an external auth server (RADIUS, SecurID, or LDAP server) that stores device administrator accounts. To select an external server from the auth server list, you must have already created and configured an Authentication Server object in the NSM UI.

By default, authentication and accounting are performed in the RADIUS auth server. You can configure separate RADIUS servers for accounting and authentication for XAuth and L2TP user types (in ScreenOS 6.2). XAUTH and L2TP users can disable the default accounting and configure a different RADIUS server for accounting.

After the device administrator is authenticated, the auth server checks the privilege level of the device admin. A privilege level defines the privileges that are accessible to the device admin after successful logging in to the device. They are:

- For device administrators stored in the local database, the security device uses the privilege level specified in the local device administrator account.
- For device administrators stored on an external auth server, select one of the following privilege settings:
  - Get privilege from RADIUS server—Select this option to query a RADIUS server for all external device administrator privileges. The RADIUS server must contain the device administrator accounts and netscreen.dct (Juniper Networks dictionary file).
  - Read-Write, Read-Only—Select a privilege level that applies to all external device administrators. Although the device administrator accounts are stored on the external server, the security device provides the device administrator privilege level. Use this option when storing accounts on a SecurID or LDAP server, or when using a RADIUS server that does not contain the Juniper Networks dictionary file. By default, the external device administrator privilege level is set to Read-Only.

**Related  
Documentation**

- [Device Administrator Account Configuration Overview on page 148](#)
- [Supporting Admin Accounts for Dialup Connections on page 151](#)

- [Importing Device Administrators from a Physical Device Overview on page 146](#)

## Device Administrator Account Configuration Overview

---

You must create an account for each device administrator on the managed device. The device administrator account contains a device admin privilege level, username, password, and optional PKA keys for the admin.

Additionally, for security devices that run ScreenOS 5.0 or later, you can configure privileges for the Trustee, such as granting the permission to configure the untrust Ethernet interface and the permission to configure the untrust modem interface.

- [Configuring Privilege Level on page 148](#)
- [Configuring Authentication on page 149](#)
- [Admin Access Lock Setting on page 150](#)
- [Roles for Device Administrator Accounts on page 151](#)

### Configuring Privilege Level

A security device supports multiple device administrators. NSM connects to the device as the root device administrator, and has complete administrative privileges for the device.

A security device can have only one root device administrator which cannot be deleted. Additionally, after you create the root device administrator (or import from an existing device) you cannot change the name of the root device administrator. To delete an existing root device administrator, you can change the privilege level of the administrator to a non-root privilege, and then save and delete the administrator. If you delete the root device administrator, however, you must then create a new root device administrator before installing the modeled configuration on the managed device (NSM must use the root device administrator account to communicate with the managed device).



**NOTE:** For ScreenOS 5.x devices, you can set or change the root device admin password using the directive “Set Root Admin.” To execute this directive, right-click the device in the Device Manager device list and select **Device > Set Root Admin**.

---

When you create other device administrators, you must assign a privilege level; these privileges are accessible to the device admin after successful log in to the device as described in [Table 31 on page 149](#).



Table 31: Privilege Level

Privilege Levels	Description
Read/Write Device Administrator	<p>The read/write administrator has the same privileges as the root device administrator, but cannot create, modify, or remove other device administrators. Privileges include:</p> <ul style="list-style-type: none"> <li>Creates virtual systems and assigns virtual system administrators</li> <li>Monitors any virtual system</li> <li>Tracks statistics (this privilege cannot be delegated to a virtual system administrator)</li> </ul>
Read-Only Device Administrator	<p>The read-only device administrator has only viewing privileges using the Web UI, and can only issue the <b>get</b> and <b>ping</b> CLI commands. Privileges include:</p> <ul style="list-style-type: none"> <li>Read-only privileges in the root system, using the following four commands: <b>enter</b>, <b>exit</b>, <b>get</b>, and <b>ping</b></li> <li>Read-only privileges in virtual systems</li> </ul> <p><b>NOTE:</b> All system administrators, including those assigned a Read-Only role, can create and run their own reports.</p>
Virtual System Device Administrator (available on security devices that support virtual systems)	<p>Each virtual system (vsys) is a unique security domain, which can be managed by virtual system device administrators with privileges that apply only to that vsys. Virtual system administrators independently manage virtual systems through the CLI or Web UI. Privileges include:</p> <ul style="list-style-type: none"> <li>Creates and edits auth, IKE, L2TP, XAuth, and Manual Key users</li> <li>Creates and edits services</li> <li>Creates and edits policies</li> <li>Creates and edits addresses</li> <li>Creates and edits VPNs</li> <li>Modifies the virtual system administrator login password</li> <li>Creates and manages security zones</li> <li>Adds and removes virtual system read-only administrators</li> </ul>
Virtual System Read-Only Device Administrator (available on security devices that support virtual systems)	<p>A virtual system read-only administrator has the same set of privileges as a read-only administrator, but only within a specific virtual system. A virtual system read-only administrator has viewing privileges for a particular vsys through the Web UI, and can only issue the <b>enter</b>, <b>exit</b>, <b>get</b>, and <b>ping</b> CLI commands within that vsys.</p>

For any configuration change made by a device administrator, the managed device generates a log entry with the name of the device administrator making the change, the IP address from which the change was made, and the time of the change. These log entries appear as configuration logs in the NSM Log Viewer.

## Configuring Authentication

A device administrator can authenticate a connection to a security device using one of two authentication methods: Password or Public Key (ScreenOS 5.x devices only). However, regardless of the authentication method you want the device administrator to use, you must initially define a password for the admin account. If you later bind a public key to the admin, the password becomes irrelevant.

Use password authentication for device administrators who need to configure or monitor the managed device. You can use this authentication method for device administrators on ScreenOS 5.x devices.



**NOTE:** All passwords handled by NSM are case-sensitive.

- To configure authentication, enter a username, password, and privilege level for the device administrator account, and then select **SSH Password Authentication**.
- To connect using an SSH-aware application, the device administrator (the SSH client) initiates an SSH connection to the managed device (the SSH server). When SSH is enabled on the interface receiving the connection request, the managed device prompts the admin for username and password, and then compares that information to the information in the device admin account. If the username and passwords match, the device authenticates the connection; if they do not match, the device rejects the connection request.

Use Public Key Authentication (PKA) for greater security or to run automated scripts. You can use this authentication method for device administrators on a ScreenOS 5.x device.

- To configure PKA, generate the PKA public/private key pair using the key generate program in an SSH client application (see the SSH client application documentation for more information). The key pair is RSA for SSHv1 and DSA for SSHv2. Assign the private key to the device administrator account, and then load the public key on the managed device using a TFTP server or SSP (ScreenOS 5.1 and later only).
- To connect using an SSH-aware application, the device administrator (the SSH client) initiates an SSH connection to the managed device (the SSH server). When SSH is enabled on the interface receiving the connection request, the managed device prompts the admin for username and public key (of a public/private key pair), and then compares that information with up to four public keys for that device admin account. If one of the keys matches, the device authenticates the connection; if no keys match, the device rejects the connection request.

When the managed device receives the connection request, it first checks the device administrator account for a public key bound to that administrator. If a matching key is found, the managed device authenticates the administrator using PKA; if no matching key is found, the managed device prompts for a username and password. You can store up to four PKA keys for each device administrator.

You must enable SSH on the interface through which the device administrator connects to the managed device using an SSH connection.

## Admin Access Lock Setting

Admin access lock configuration locks out the administrator who fails to authenticate before the configured timeout from the specified account. If this option is disabled, you cannot set the authentication failure length and the default value is set to 1. If this option

is enabled, you can set the admin access locking time to lock out the account. The lockout occurs after the specified number of failed login attempts.

## Roles for Device Administrator Accounts

You can configure role attributes for admin users. If you select the privilege of admin user as root, you cannot set the role attribute (that is, the root administrator cannot set role attributes.) If you set privilege as read-write or read-only, you can assign any of the available role attributes. The default value is Not Assigned.

### Related Documentation

- [Supporting Admin Accounts for Dialup Connections on page 151](#)
- [Restricting Management Connections Using Permitted IPs on page 152](#)
- [Device Administrator Authentication Overview on page 147](#)

---

## Supporting Admin Accounts for Dialup Connections

The NetScreen-5XT and the NetScreen-5GT devices support a modem connection for outbound dial-up disaster recovery situations. You can set up trustee accounts for the interface or for the modem. This topic describes the two types of trustees:

- Interface trustee

An interface trustee has access only to the Untrust interface through the Web UI. An interface trustee can only assign the IP address for the primary Untrust zone interface. Also, an interface trustee account can enable or disable ping responses from an interface. Interface trustees can select either a PPPoE or DHCP client using automatic IP address assignment or a static address assignment client.

- Modem trustee

A modem trustee can access, configure, and modify only the ISP1 and ISP2 settings. A modem trustee can also test and view the configurations for the ISP3 and ISP4 settings.

You can configure Modem Trustee and Interface Trustee accounts to have Read/Write or Read-Only levels of access.

The connection type to a device by a Trustee administrative account occurs exclusively, preventing any other connection type from occurring. The secure trustee connection prevents local console, Telnet, and SSH sessions to connect to the device if these other connection types attempt to use the trustee's name or password.

### Related Documentation

- [Restricting Management Connections Using Permitted IPs on page 152](#)
- [Local Access Configuration Using CLI Management Overview on page 153](#)
- [Device Administrator Account Configuration Overview on page 148](#)

## Restricting Management Connections Using Permitted IPs

---

Use permitted IPs to restrict management connections (a connection in which a device administrator attempts to log in) to specific IP addresses. By default, any host on the trust interface of the managed device can connect to the security device and attempt to log in. You can configure the device to permit management connections from one or more user-defined IP addresses only.

After you create permitted IPs (and update the device with the modeled configuration), the device immediately begins rejecting management connections from nonpermitted IP addresses. If a device administrator is managing the device using a remote network connection and the workstation is not included as a permitted IP, the security device immediately terminates the device administrator's session.

To create a permitted IP, click the **Add** icon in the Permitted IP area, and then configure an IP address and netmask.



**NOTE:** Configuring a permitted IP for a device administrator does not affect the NSM-managed device connection.

---

Corporation A has a small network in which a single device administrator at 172.16.40.42 is allowed to manage the security device. For this device, you create a permitted IP with an IP/netmask of 172.16.41.42/32.

Corporation B has a large network with multiple devices. Several device administrators on the 172.16.40.0 subnet require access to all devices. For each device, you create a permitted IP with an IP/netmask of 172.16.40.0/24.

On devices running ScreenOS 6.3, permitted IPs used for restricting management connections supports IPv6.

### Related Documentation

- [Local Access Configuration Using CLI Management Overview on page 153](#)
- [File Formatting in NSM Overview on page 153](#)
- [Supporting Admin Accounts for Dialup Connections on page 151](#)

---

## Local Access Configuration Using CLI Management Overview

---

Use the CLI management options to configure local access using a console connection, or remote access using Telnet or SSH. A device administrator can connect directly to most security devices using the console port. CLI management settings apply to all device administrators for the security device.

Additionally, to manage a device remotely using Telnet or SSH, the device administrator must use a permitted IP address to initiate a Telnet or SSH connection to the device, and the correct service option must be enabled for the interface that the device administrator connects to on the device. For details on configuring permitted IP addresses, see [“Restricting Management Connections Using Permitted IPs” on page 152](#); for details on configuring service options for a device interface, see the *Network and Security Manager Administration Guide*.

### Related Documentation

- [File Formatting in NSM Overview on page 153](#)
- [Port Numbers for SSH and Telnet Connections in NSM Overview on page 154](#)
- [Restricting Management Connections Using Permitted IPs on page 152](#)

---

## File Formatting in NSM Overview

---

The file format determines the format (DOS or UNIX) of device configuration files. The CLI commands that configure the security device are automatically stored in a text-based configuration file. Occasionally, for troubleshooting purposes, a device administrator might need to view this configuration file outside of the security device.

To configure the file format of the configuration file, select the format that matches the computer system on which the configuration files will be viewed:

- In a UNIX text file, a line of text is terminated by a line-feed character. When viewing a UNIX text file on a UNIX or DOS-based system, this line feed character does not appear. If you typically view configuration files on a UNIX system, select **UNIX** as the file format.
- In a DOS text file, a line of text is terminated by a line-feed and a carriage return (^M). When viewing a DOS text file on a UNIX system, the carriage return character appears onscreen. If you typically view configuration files on a DOS-based system, select **DOS** as the file format.

### Related Documentation

- [Port Numbers for SSH and Telnet Connections in NSM Overview on page 154](#)
- [Limiting Login Attempts, Setting Dial-In Authentication, and Restricting Password Length in NSM Overview on page 154](#)
- [Local Access Configuration Using CLI Management Overview on page 153](#)

## Port Numbers for SSH and Telnet Connections in NSM Overview

---

You can configure the port numbers to use for SSH and Telnet connections:

- The default port for SSH client connections is 22; to change this default, enter a port number between 1024 and 32,767.
- The default port for Telnet client connections is 23; to change this default, enter a port number between 1024 and 32,767.

In a vsys system, the root and vsys share the same SSH port number. For example, if you change the SSH port from the default port 22, the port is also changed for all vsys.



**NOTE:** For ScreenOS 5.x devices, you can set or change the device port numbers that accept Telnet and/or SSH connections the “Set Admin Ports” directive. To execute this directive, right-click the device in the Device Manager device list and select **Device > Set Admin Ports**.

### Related Documentation

- [Limiting Login Attempts, Setting Dial-In Authentication, and Restricting Password Length in NSM Overview on page 154](#)
- [Asset Recovery and Reset Hardware in NSM Overview on page 155](#)
- [File Formatting in NSM Overview on page 153](#)

## Limiting Login Attempts, Setting Dial-In Authentication, and Restricting Password Length in NSM Overview

---

This topic describes the information about how to limit login attempts, set dial-in authentication, and restrict password length and they are as follows:

### Configuring Connection Attempts

To minimize unauthorized access, you can limit the number of unsuccessful login attempts allowed before the security device terminates a Telnet session. This restriction also protects against certain types of attacks, such as automated dictionary attacks.

By default, a security device allows up to three unsuccessful login attempts before it closes the Telnet session.

### Configuring Modem Dial-In Authentication Timeout

You can set dial-in authentication timeout. You can even set the timeout as never time out for users who dialin.

### Configuring Password Length Restriction

To prevent a root device administrator from using short passwords (which are easier to decode and discover), you can set the minimum length requirement for the root device administrator password to any number from 1 to 31.

However, to set this restriction, the current root device administrator password must meet the minimum length requirement you are attempting to set. If the current password is too short, NSM displays an error message.

**Related Documentation**

- [Asset Recovery and Reset Hardware in NSM Overview on page 155](#)
- [Console-Only Connections in NSM Overview on page 156](#)
- [Port Numbers for SSH and Telnet Connections in NSM Overview on page 154](#)

## Asset Recovery and Reset Hardware in NSM Overview

If the root device administrator password is lost, the device administrator can restore access in one of two ways as described in [Table 32 on page 155](#).

**Table 32: Asset Recovery and Reset Hardware**

Restore Access Methods	Description
Using Asset Recovery	<p>Using a console connection, the device administrator uses the <b>unset all</b> command to clear all existing configuration settings and return the device to factory defaults (for details, see the "Administration" volume in the <i>Concepts &amp; Examples ScreenOS Reference Guide</i>). Device recovery is enabled by default. To disable it, clear the <b>Enable Asset Recovery</b> check box in the CLI Management configuration screen.</p> <p><b>NOTE:</b> A security device in FIPS mode automatically disables asset recovery.</p>
Reset Hardware	<p>The device administrator performs a manual operation on the physical device hardware to return the device to factory defaults (for details, see the "Administration" volume in the <i>Concepts &amp; Examples ScreenOS Reference Guide</i>). Reset Hardware is enabled by default. To disable it, clear the <b>Enable Reset Hardware</b> check box in the CLI Management configuration screen.</p>

All configuration settings stored on the managed device are lost during an asset recovery or hardware reset. After restoring access to the device, the device administrator should perform the following tasks to enable the device to reconnect to NSM:

1. Configure the interface that connects to the management system.
2. Send the new root device administrator username and password to the NSM administrator, who should update the existing root username and password for the device in the modeled configuration.



**NOTE:** All passwords handled by NSM are case-sensitive.

3. Enable the NSM agent on the managed device.

After the device has reconnected to the management system, you (the NSM administrator) can update the device with the modeled configuration.

**Related Documentation**

- [Console-Only Connections in NSM Overview on page 156](#)
- [Secure Shell Server in NSM Overview on page 156](#)

- [Limiting Login Attempts, Setting Dial-In Authentication, and Restricting Password Length in NSM Overview on page 154](#)

## Console-Only Connections in NSM Overview

---

You can require the root device administrator to log in to the security device through the console port only. This restriction requires the root device admin to have physical access to the device to log in, preventing unauthorized persons from logging in remotely.

By default, this restriction is not enabled (the root device administrator can log in remotely). To restrict access to console only, select the **Root Access Console Only** check box in the CLI Management screen. When enabled, the managed device denies access to all Web UI, Telnet, or SSH connections for the root device administrator. This setting overrides the management options enabled on the ingress interface.



**NOTE:** This option does not appear for the Juniper Networks NSMXpress, which does not contain a console port.

Enabling the console-only setting does not affect the NSM-managed device connection.

### Related Documentation

- [Secure Shell Server in NSM Overview on page 156](#)
- [Configuring CLI Banners in NSM Overview on page 158](#)
- [Asset Recovery and Reset Hardware in NSM Overview on page 155](#)

## Secure Shell Server in NSM Overview

---

Each security device includes a built-in Secure Shell (SSH) server. Device administrators can use an SSH-aware application to open a remote command shell on the device and execute commands. When using SSH, the connection is protected against IP or DNS spoofing attacks, and password or data interception.

The maximum number of SSH sessions is a device-wide limit and is between 2 and 24, depending upon the device. If the maximum number of SSH clients are already logged into the device, no other SSH client can log in to the SSH server.

To enable SSH connections to the managed device, select **SSH Enable** and configure an SSH version. Because SSHv1 and SSHv2 are incompatible, you must use the same SSH version for both the client and server. For example, you cannot use an SSHv1 client to connect to an SSHv2 server on the managed device, or vice versa.

For the SSH server (the security device), you can also enable Secure Copy (SCP). A device administrator can use SCP to transfer files to or from the managed device using SSH (SSH authenticates, encrypts, and ensures data integrity for the SCP connection). When using SCP, the security device acts as an SCP server that accepts connections from SCP clients on remote hosts. Additionally, you must enable SSH for the managed device before you can enable SCP (disabled by default).





**NOTE:** For ScreenOS 5.x devices, you can enable or disable SSH for device admin connections using the directive “Set Admin SSH.” To execute this directive, right-click the device in the Device Manager device list and select **Device > Set Admin SSH**.

- [Using SSH Version 1 \(SSHv1\) on page 157](#)
- [Using SSH Version 2 \(SSHv2\) on page 157](#)

## Using SSH Version 1 (SSHv1)

SSHv1 is widely deployed and is commonly used. You can use a password or Public Key Authentication (PKA) to authenticate an SSHv1 connection.

When using PKA authentication for the SSHv1 server (the security device) you can also set the key generation interval for the host PKA key. When you enable SSH on a managed device, the device generates a unique host key that is permanently bound to the device (each vsys has its own host key). If SSH is disabled, then enabled again, the device uses the same host key. The security device uses the host key to identify itself to an SSH client (device administrator).

After the key is generated, it can be distributed to the SSH client in one of two ways:

- **Manually**—Send the host key to the client admin user through e-mail or phone. The device administrator stores the host key in the appropriate SSH file on the SSH client system (the SSH client application determines the file location and format).
- **Automatically**—When the SSH client connects to the managed device, the SSH server sends the unencrypted public component of the host key to the client. The SSH client searches its local host key database to see if the received host key is mapped to the address of the security device. If the host key is unknown (there is no mapping to the device address in the client’s host key database), the device admin user can accept the host key and authenticate the connection, or reject the host key and terminate the connection request.

To configure the SSH client, you must also bind the RSA PKA keys to the device administrator before that admin can make an SSH connection. For details on assigning PKA keys to a device admin, see [“Device Administrator Account Configuration Overview” on page 148](#).



**NOTE:** NSM supports PKA keys for device administrator authentication only for devices running ScreenOS 5.x.

## Using SSH Version 2 (SSHv2)

SSHv2 is considered more secure than SSHv1 and is currently being developed as the IETF standard.

To configure the SSH client, you must also bind the DSA PKA keys to the device administrator before that admin can make an SSH connection. For details on assigning PKA keys to a device admin, see [“Device Administrator Account Configuration Overview” on page 148](#).

**Related  
Documentation**

- [Configuring CLI Banners in NSM Overview on page 158](#)
- [Configuring Remote Access Using Web Management Overview on page 159](#)
- [Console-Only Connections in NSM Overview on page 156](#)

---

## Configuring CLI Banners in NSM Overview

You can customize the message that appears when a device administrator logs on to the security device using a console connection, Telnet, or SSH. This message, called a banner, provides confirmation to device administrators to let them know that they have successfully logged in. Banners are optional; you are not required to configure CLI banners for the security device.

A default banner already exists for Telnet and SSH, but you can write a new message to suit your needs. You can use one banner for console connection and a different banner for both Telnet and SSH connections.

To configure CLI banners:

- For console connections, enter a message in the Console Login Banner text box. By default, the console banner is blank (no confirmation is provided to the device administrator upon successful login). The maximum number of characters permitted in a console banner is 127.
- For Telnet or SSH connections, enter a new message or edit the existing default message in the Telnet/SSH Login Banner text box. By default, the message “Remote Management Console” is provided to device administrators upon successful login. The maximum number of characters permitted in a Telnet or SSH banner is 127.

For ScreenOS 5.1 and later devices, you can also configure a secondary banner for console, Telnet, or SSH connections. The secondary banner enables you to create a much longer message that appears for any successful CLI-based connection attempt. By default, the secondary banner is blank (no secondary message is provided for device administrators upon login).

In ScreenOS 6.1, for sessions created through ssh, telnet, or local console, the secondary banner gets displayed after the username and the password prompt. These actions can request the administrator to acknowledge the secondary banner through the CLI console. Hence, if the user does not acknowledge the secondary banner, the device login process fails and the connection is closed.

**Related  
Documentation**

- [Configuring Remote Access Using Web Management Overview on page 159](#)
- [Configuring HTTP Administrative Connections in ScreenOS Devices Using NSM Overview on page 159](#)

- [Secure Shell Server in NSM Overview on page 156](#)

---

## Configuring Remote Access Using Web Management Overview

---

Use the Web management options to configure remote access using the Hypertext Transfer Protocol (HTTP). A device administrator can use a standard Web browser and HTTP to remotely access the Web UI on the security device. Web management settings apply to all device administrators for the security device.

Additionally, to manage a device using the Web UI, the device administrator must use a permitted IP address to initiate an HTTP connection to the device, and the correct service option must be enabled for the interface that the device administrator connects to on the device. For details on configuring permitted IP addresses, see [“Restricting Management Connections Using Permitted IPs” on page 152](#); for details on configuring service options for a device interface, see [“Enabling Management Service Options for Interfaces” on page 56](#).

### Related Documentation

- [Configuring HTTP Administrative Connections in ScreenOS Devices Using NSM Overview on page 159](#)
- [Configuring Secure Connections in ScreenOS Devices Using NSM Overview on page 160](#)
- [Configuring CLI Banners in NSM Overview on page 158](#)

---

## Configuring HTTP Administrative Connections in ScreenOS Devices Using NSM Overview

---

You can configure the following options for administrative connections that use HTTP:

- Idle time for Web UI management—The number of seconds that the HTTP connection remains idle (no traffic is flowing) before the device drops the connection.
- Port number—The default HTTP port number is 80. If you are running HTTP services on a different device port, enter that port number here.

Additionally, the device administrator must use a permitted IP address to initiate an HTTP connection to the device, and the Web service option must be enabled for the interface that the device administrator connects to on the device.

To secure HTTP administrative traffic, you can use the Secure Sockets Layer (SSL) protocol.

### Related Documentation

- [Configuring Secure Connections in ScreenOS Devices Using NSM Overview on page 160](#)
- [Configuring Network Time Protocol and NTP Backup Server in NSM Overview on page 161](#)
- [Configuring Remote Access Using Web Management Overview on page 159](#)

## Configuring Secure Connections in ScreenOS Devices Using NSM Overview

Secure Sockets Layer (SSL) is a set of protocols that can provide a secure connection between a Web client and a Web server communicating over a TCP/IP network. SSL consists of the SSL Handshake Protocol (SSLHP), which enables a client and server to authenticate each other and negotiate an encryption method, and the SSL Record Protocol (SSLRP), which provides basic security services to higher level protocols such as HTTP. Using certificates, SSL authenticates the server (the security device), and then encrypts the traffic sent during the session. Juniper Networks supports authentication only of the server (the security device), not the client (the device administrator); the device authenticates itself to the device administrator, but the device administrator does not use SSL to authenticate to the device. However, the device administrator must connect using a Web browser with SSL version 3 compatibility (not version 2). Netscape Communicator 4.7x and later and Internet Explorer 5.x and later are SSL version 3 compatible.

During the SSL handshake, the security device sends the device administrator its self-signed certificate. The device admin encrypts a random number with the public key contained in the certificate and sends the number back to the device, which uses its private key to decrypt the number. Both participants then use the shared random number and a negotiated secret key cipher (3DES, DES, RC4, or RC4-40) to create a shared secret key, which they use to encrypt traffic between themselves. They also use an agreed-upon compression method (PKZip or gzip) to compress data and an agreed-upon hash algorithm (SHA-1, SHA-2, or MD5) to generate a hash of the data to provide message integrity.

Additionally, the device administrator must use a permitted IP address to initiate an HTTP connection to the device, and the SSL service option must be enabled for the interface that the device administrator connects to on the device.

By default, SSL is disabled. To ensure that all HTTP connections to the Web UI are secure, you should enable this option. When enabled, the device automatically redirects administrative traffic using HTTP (default port 80) to HTTPS (SSL, default port 443) and authenticates using the local certificate. For a device running ScreenOS 5.1 and later, SSL uses the autogenerated, self-signed certificate on the device.

You can change the SSL configuration by editing the SSL settings as described in [Table 33 on page 160](#).

**Table 33: SSL Settings**

SSL Settings	Your Action
Redirect HTTP to HTTPS	You can enable HTTP redirection for SSL troubleshooting, if desired.
Certificate	By default, the security device uses an auto-generated self-signed certificate for SSL. To change the certificate used for SSL, select a certificate from the list of available certificates.
Port	The default port for SSL connections is 443; to change this default, enter a different port number.

Table 33: SSL Settings (*continued*)

SSL Settings	Your Action
Cipher	<p>Select an encryption algorithm for SSL:</p> <ul style="list-style-type: none"> <li>• RC4-40 with 40-bit keys</li> <li>• RC4 with 128-bit keys</li> <li>• DES: Data Encryption Standard with 56-bit keys</li> <li>• 3DES: Triple DES with 168-bit keys</li> </ul> <p>The RC4 algorithms are paired with MD5; DES and 3DES with SHA-1.</p>
Authentication	<p>Select an authentication method for SSL:</p> <ul style="list-style-type: none"> <li>• Message Digest version 5 (MD5)—128-bit keys</li> <li>• Secure Hash Algorithm version 1 (SHA-1)—160-bit keys</li> <li>• Secure Hash Algorithm version 2 (SHA-2)—256-bit keys</li> </ul>

While SSL is enabled, any device administrator can connect to the security device using the SSL port. When administrative connections use SSL, in the Web browser URL field, the device admin must enter the https (instead of http) before the IP address used to manage the device. If you changed the default SSL port from 443, the device administrator must also append a colon and the SSL port number to the IP address. For example, to connect to the 5.5.5.5 interface and SSL port 1443, the device administrator must enter **https://5.5.5.5:1443**.

To use HTTP without SSL, disable SSL by clearing the **Enable SSL** check box. The device no longer redirects HTTP connections to SSL, and no authentication occurs for the connection.

#### Related Documentation

- [Configuring Network Time Protocol and NTP Backup Server in NSM Overview on page 161](#)
- [Setting ScreenOS Authentication Options Using General Auth Settings on page 163](#)
- [Configuring HTTP Administrative Connections in ScreenOS Devices Using NSM Overview on page 159](#)

## Configuring Network Time Protocol and NTP Backup Server in NSM Overview

Use the Date/Time option to configure date and time synchronization on security devices. The date and time setting on the device affects VPN tunnel setup and schedule objects used in active security policies.

You configure the device time in relation to GMT.

- [Configuring Network Time Protocol on page 162](#)
- [Configuring an NTP Backup Server on page 162](#)

## Configuring Network Time Protocol

To ensure that the security device always maintains the right time, the device can use Network Time Protocol (NTP) to synchronize its system clock with that of an NTP server on the Internet.

To use NTP, first enable Network Time Protocol, and then configure the settings as described in [Table 34 on page 162](#).

**Table 34: Network Time Protocol Settings**

NTP Settings	Your Action
Synchronization	You can configure the security device to perform this synchronization automatically at time intervals that you specify. By default, the synchronization interface is set to 10 minutes, with a 3 second maximum adjustment threshold.
Authentication	<p>You can secure NTP traffic by enabling authentication. When using authentication, for each NTP server you configure on the security device, you must assign a unique server key ID and preshare key; the key ID and preshare key serve to create an MD5 checksum, with which the device and the NTP server can authenticate NTP data. Select the authentication mode that the device uses when connecting to an NTP server:</p> <ul style="list-style-type: none"> <li>• <b>Required</b>—The device must include the authentication information—server key ID and MD5 checksum—in every packet it sends to an NTP server and must authenticate all NTP packets it receives from an NTP server. If authentication fails, the device denies NTP traffic from the NTP server.</li> <li>• <b>Preferred</b>—The device attempts to authenticate NTP traffic using the same methods as the Required options but continues to send and receive NTP traffic if authentication fails.</li> <li>• <b>None (default mode)</b>— Select this mode if you do not want to authenticate NTP packets.</li> </ul>
NTP Servers	You can configure up to three NTP servers (one primary and two backups) from which the security device can regularly update its system clock. If you enable authentication by selecting the Required or Preferred authentication options, you must also provide a unique server key ID and preshare key for each NTP server that you configure.

## Configuring an NTP Backup Server

You can specify an individual interface as the source address to direct Network Time Protocol (NTP) requests from the device over a VPN tunnel to the primary NTP server or a backup server as necessary. Among other interface types, you can select a loopback interface to perform this function.

The security device sends NTP requests from a source interface and optionally uses an encrypted preshared key when sending NTP requests to the NTP server. The encrypted preshared key provides authentication.

- Related Documentation**
- [Setting ScreenOS Authentication Options Using General Auth Settings on page 163](#)
  - [Setting ScreenOS Authentication Options Using Banners Overview on page 164](#)
  - [Configuring Secure Connections in ScreenOS Devices Using NSM Overview on page 160](#)

## Setting ScreenOS Authentication Options Using General Auth Settings

The authentication screens contain the following device-wide authentication options you can configure on a security device.

For devices running ScreenOS 5.2, you can configure some general settings that determine how the security device handles authentication session cleanup and authentication requests.

- [Clearing RADIUS Sessions on page 163](#)
- [Assigning an Authentication Request Interface on page 163](#)

### Clearing RADIUS Sessions

Occasionally, overcharging can occur when a wireless user is assigned the same IP address that was used for a previously closed connection by a different user. Because the IP addresses are the same for both connections, the first wireless user might be charged for the second user's connection time. You can prevent this problem by configuring the security device to clear RADIUS sessions for a specific IP address when the RADIUS accounting-stop message is received for that connection.

To enable session cleanup for a security device, in the device navigation tree, select **Auth > General**. Configure a RADIUS Accounting Listener port that monitors the connection for accounting-stop messages, and then select the option **RADIUS Accounting Cleanup Action: Session Cleanup**.

### Assigning an Authentication Request Interface

By default, the security device sends authentication requests using the route defined in the route table. For devices running ScreenOS 5.2, you can configure a specific outgoing source interface for requests sent to an authentication server. You might need to specify a specific interface for auth requests destined for a VPN tunnel or to route all auth requests through the same interface for authentication monitoring.

To configure a source interface, in the device navigation tree, select **Auth > General**, and then click the **Add** icon in the Source Interface used for Outgoing Auth Request area. Select the Authentication Server object that represents the authentication server receiving the request, and then select an interface on the device through which requests are sent.



**NOTE:** For details on configuring Authentication Server objects, see the *Network and Security Administration Guide*.

After you specify a source interface for auth requests, the security device routes all auth requests destined for a RADIUS, LDAP, or SecurID server through that interface (one source interface per authentication server object).

#### Related Documentation

- [Setting ScreenOS Authentication Options Using Banners Overview on page 164](#)
- [Setting ScreenOS Authentication Options Using Default Servers Overview on page 165](#)

- [Configuring Network Time Protocol and NTP Backup Server in NSM Overview on page 161](#)

## Setting ScreenOS Authentication Options Using Banners Overview

You can customize the message that appears when a device user logs on to the security device through Telnet, FTP, HTTP, or WebAuth. This message, called a banner, provides confirmation to device users to let them know the status of the connection. Default banners already exist, but you can write a new message to suit your needs. You can use different banners for each protocol.



**NOTE:** To configure the Telnet, SSH, or console connection banner, see [“Configuring CLI Banners in NSM Overview” on page 158](#).

To configure a protocol banner, select the protocol tab and edit the default Telnet, FTP, and HTTP messages as described in [Table 35 on page 164](#).

**Table 35: Protocol Banner Settings**

Protocol Banner Settings	Your Action
Attempted Logins	Enter a new message or edit the existing default message in the Login text box. Device users receive this message when they are prompted for their authentication credentials.
Successful Logins	Enter a new message or edit the existing default message in the Success text box. Device users receive this message after their credentials have been authenticated and a connection has been established.
Failed Logins	Enter a new message or edit the existing default message in the Fail text box. Device users receive this message when authentication fails or when the device user is not authorized to access the device.

To configure the WebAuth banner, select the **WebAuth** tab and enter a new message (or edit the existing default message in the Success text box. This message is provided to auth user when their WebAuth credentials have been authenticated and a connection has been established. The message appears at the top of a Web browser screen, after an auth user has successfully logged on to a WebAuth address. Typically, the message informs the user that the authentication was successful, but you can enter any message you want, up to a maximum of 220 characters.

Banners are optional; you are not required to configure banners for the security device.



**NOTE:** Device administrators can create login banners for console, telnet, and secondary connections.

### Related Documentation

- [Setting ScreenOS Authentication Options Using Default Servers Overview on page 165](#)
- [Setting ScreenOS Authentication Options Using General Auth Settings on page 163](#)



- [Setting ScreenOS Authentication Options Using Infranet Settings Overview on page 165](#)

## Setting ScreenOS Authentication Options Using Default Servers Overview

The default servers for the security device define the authentication servers used to provide local, external, and WebAuth user authentication. [Table 36 on page 165](#) describes the different default servers.

**Table 36: Default Servers**

Default Servers	Description
Local	<p>Each security device contains a local (database) server called auth server. The auth server is the default authentication server and can handle all types of authentication that occur on the device. Usernames and authentication credentials of all local users are stored in this database.</p> <p>For the Local server only, you can set the authentication timeout, which is the number of minutes the connection remains active after an authentication request has been submitted and a successful authentication is received. By default, the authentication timeout on the Local authentication server is 10 minutes. To change this timeout, enter a new value.</p>
External	<p>Alternatively, you can select an external authentication server as the default server. To select an external server, you must have already created and configured an Authentication Server object in the NSM UI. You must also have defined the user accounts for all external users on the external server. For more information, see the <i>Network and Security Manager Administration Guide</i>.</p>
WebAuth	<p>When using WebAuth, an auth user first initiates an HTTP session to the IP address of the security device that hosts WebAuth. After successful authentication, the auth user can send traffic to the destination as permitted by one or more security policies. To authenticate WebAuth users, you can use the Local authentication server (security device default) or select a previously defined external auth server.</p>

- Related Documentation**
- [Setting ScreenOS Authentication Options Using Infranet Settings Overview on page 165](#)
  - [General Report Settings for ScreenOS Devices Overview on page 166](#)
  - [Setting ScreenOS Authentication Options Using Banners Overview on page 164](#)

## Setting ScreenOS Authentication Options Using Infranet Settings Overview

If you have deployed Juniper Networks Infranet Controllers as part of your network security infrastructure, you can use the Infranet Settings screen on devices running ScreenOS 5.3 and later to configure the properties as described in [Table 37 on page 165](#).

**Table 37: Infranet Settings**

Infranet Settings	Description
Contact Interval	The time interval (in seconds) that the Infranet Enforcer waits before attempting to connect to the next available Infranet Controller; the default interval is set to 10 seconds.

Table 37: Infranet Settings (*continued*)

Infranet Settings	Description
Action on Timeout	For any reason, if your connection to the Infranet Controller times out, the device terminates the SSH connection and clears all Infranet Controller related context. You can change this behavior by setting the timeout action to "Open," in which case the Infranet Enforcer allows all traffic; or "No Change," in which case the Infranet Enforcer preserves the current state of all existing tunnel sessions.
Enforcer Mode	This setting takes the Infranet Enforcer out of regular mode and into Test mode. Test mode is recommended before you actually deploy the Infranet Enforcer enabling you to evaluate how the solution works. In this mode, the Infranet Enforcer allows all traffic that matches the Infranet policy. Logs are created indicating the behavior of the Infranet Enforcer as if it were operating in Regular mode.
Infranet Controllers	<p>You can configure up to eight (8) Infranet Controllers. The order in which these are entered is used by the Infranet Enforcer to contact each Infranet Controller. Devices permit only one redirect URL per Infranet Controller.</p> <p>In devices running ScreenOS 6.2 or later, when UAC is deployed through a ScreenOS firewall, the firewall acts as the Infranet Enforcer and redirects unauthorized access to a configured URL (captive portal). The device configures the redirect URL through a policy, which means that more than one redirect URL can be configured for the same Infranet Controller.</p>

You can also configure security devices to authenticate using Infranet Controllers in a rule in a security policy. Refer to the *Network and Security Manager Administration Guide* for more information.

#### Related Documentation

- [General Report Settings for ScreenOS Devices Overview on page 166](#)
- [Configuring Syslog Host Using NSM \(NSM Procedure\) on page 167](#)
- [Setting ScreenOS Authentication Options Using Default Servers Overview on page 165](#)

## General Report Settings for ScreenOS Devices Overview

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

For information about configuring reporting settings, "[General Report Settings for ScreenOS Devices Overview](#)" on page 166.

For more information about reporting concepts for the security devices, see the "Administration" volume in the *Concepts & Examples ScreenOS Reference Guide*.

Use the General Report settings to configure the severity levels of the messages you want to log and where you want those messages sent. As of ScreenOS 6.3, there are about nine destinations for log messages. You can enable or disable the option to include serial numbers in log messages. Each system event on a security device is assigned a level of severity. By default, packets that are dropped on the security device are logged to the self log. In the Firewall Options, you can disable or enable logging of dropped packets for specific traffic types, including ICMP, IKE, SNMP, and multicast packets.

You can also use this tab to set thresholds determining how many packets of a particular type the packet process unit (PPU) sends to the CPU per second, before dropping subsequent packets of that type. The PPU is a hardware processor in some security device systems that forwards packets to the flow CPU. Enabling PPU packet drop thresholds adds an extra layer of DoS-attack protection to the device, similar to SYN-cookie and SYN-proxy. PPU protection prevents DoS attacks from overwhelming the flow CPU, keeping the CPU responsive to critical tasks even under heavy traffic. PPU protection processes three categories of traffic: packets that do not use the IP protocol; packets carrying contents other than TCP or UDP; and system-critical IP packets, including BGP, OSPF, RIP, SNMP, system management, SIP, and H323 traffic. [Table 38 on page 167](#) describes the general report settings.

**Table 38: General Report Settings**

Report Settings	Function
Email Notification Settings	Configures a device to send messages using e-mail whenever a system event of Emergency, Alert, Critical, or Notification severity level occurs. To configure e-mail notification, you must specify the SMTP mail server and at least one e-mail address; if desired, you can enter a secondary e-mail address as well.
NSM Reporting	Configures a device to report specified events to NSM. You configure the primary IP address of the NSM Device Server and select the categories of events that are tracked on the security device and reported to NSM. You can also set the interval at which the NSM device server polls for policy statistics and protocol distribution events.
SNMP Reporting	<p>Configures the Simple Network Management Protocol (SNMP) agent for a device. The SNMP agent provides a view of statistical data about the network, the devices in it, and system events of interest.</p> <p>You also must enable SNMP manageability on the interface through which the applicable SNMP manager communicates with the SNMP agent in the security device.</p>
Syslog Reporting	Configures a device to generate syslog messages for system events at predefined severity levels. It also generates messages for all event and traffic log entries that the security device can store internally. It sends these messages over 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 use to send syslog packets.

- Related Documentation**
- [Setting ScreenOS Authentication Options Using Infranet Settings Overview on page 165](#)
  - [Configuring Syslog Host Using NSM \(NSM Procedure\) on page 167](#)

## Configuring Syslog Host Using NSM (NSM Procedure)

To configure syslog hosts using NSM:

1. Click the **Add** icon in the Syslog configuration screen. The host configuration dialog box appears.
2. Specify the hostname and the port to which the security device sends syslog messages.
3. For each syslog host, you specify the following:

- Whether the security device includes traffic log entries, event log entries, or both traffic and event log entries
  - The security facility, which classifies and sends messages to the Syslog host for security-related actions; and the regular facility, which classifies and sends messages for events unrelated to security
  - Which transport protocol (UDP or TCP) is used for sending syslog messages
4. Click **OK**.
  5. Use WebTrends reporting to configure a device to send syslog reports to a WebTrends Syslog host. WebTrends Firewall Suite enables you to customize syslog reports to display the information you want in a graphical format.

To configure the security device to send syslog reports to a WebTrends Syslog host, you first enable WebTrends reporting, and then specify the name of the WebTrends host and the port on which the syslog messages are sent. If you are sending reports through a VPN tunnel, click **Use Trust Zone Interface**.

As of ScreenOS 6.3, the event log, traffic log, and IDP log formats follow the WebTrends Enhanced Format (WELF) log regulation. If backup for the logs is enabled, logs can be sent to a maximum of four WebTrends servers. TCP or UDP transport protocol can be used for communication. IP connections can be manually reset.

For more details on configuring these reporting options, see the *Network and Security Manager Administration Guide*.

**Related  
Documentation**

- [Configuring SNMPv3 in ScreenOS Devices \(NSM Procedure\) on page 168](#)
- [General Report Settings for ScreenOS Devices Overview on page 166](#)

---

## Configuring SNMPv3 in ScreenOS Devices (NSM Procedure)

---

The Simple Network Management Protocol (SNMP) agent for a Juniper Networks security device provides network administrators with a way to view statistical data about the network and the devices on it and to receive notification of system events of interest.

Juniper Networks security devices support SNMPv1, SNMPv2c, and SNMPv3. Security devices are not shipped with a default configuration for SNMPv3. To configure your security device for SNMPv3, you must first create a unique engine ID to identify an SNMP entity and a user-based security model (USM) with the respective privilege and password. By default, the SNMPv3 engine ID is the serial number of the device.

When you create a USM, you can specify the authentication type (MD5, SHA, or None). The authentication type computes identical message digests for the same block of data. The USM requires a password and uses Data Encryption Standard (DES) to encrypt and decrypt the SNMPv3 packets.

To configure SNMPv3 features in ScreenOS devices:

1. In the NSM navigation tree, select **Device Manager > Devices**. The Device Tree page appears.
2. Click the **Device Tree** tab, and then double-click the security device for which you want to configure SNMPv3 features.
3. In the Configuration page, select **Report Settings > SNMPv3**. The SNMPv3 page appears.
4. Add or modify the SNMPv3 features as described in [Table 39 on page 169](#).
5. Click one:
  - **OK**—Saves the changes.
  - **Cancel**—Cancels the modifications.

**Table 39: Configuring SNMPv3 Features in ScreenOS Devices**

Option	Description
<b>SNMPv3 &gt; Basic tab</b>	
Local Engine ID	Identifies an SNMP entity and a USM with the respective privilege and password.
<b>SNMPv3 &gt; USM User tab</b>	
User Name	Specifies the username of the USM.
Auth Protocol	Specifies an authentication type. Select a value from the drop-down list. When you select either MD5 or SHA, you are prompted to enter an authentication password.
<b>SNMPv3 &gt; View tab</b>	
View Name	Specifies the view name of the model. Each view is tagged with an object identifier (OID) and mask values.
Oid	Specifies the object identifier. The format to enter an OID: Begin with "." and separate by ".". For example, .3.4.5.2
Mask	Specifies the mask values of the view model. You can enter a two-digit value only.
Type	Specifies if you want to include or exclude an IP address entry from the address list of the MIB tables.
<b>SNMPv3 &gt; Access Group tab</b>	
Group	Specifies the access group name.
Security Model	Specifies the security model for the access group.
Security Level	Specifies the security level for the access group.
Notify	Specifies the notification parameter for the access group.
Read	Specifies the read access privilege for the access group.
Write	Specifies the write access privilege for the access group.

**Table 39: Configuring SNMPv3 Features in ScreenOS Devices (*continued*)**

<b>SNMPv3 &gt; Community tab</b>	
Community Name	Specifies the community name that is in combination with an access group.
Tag	Specifies the tag name. Each community is tagged.
<b>SNMPv3 &gt; Sec-to-group Mapping tab</b>	
Group	Specifies the group name of the group section map.
Security Model	Specifies the security model of the group section.
Mapping User	Specifies the username that is mapped with the USM.
<b>SNMPv3 &gt; Filter tab</b>	
Filter Name	Specifies the filter name. A security device can support up to 32 SNMPv3 filters.
Oid	Specifies the object identifier. The format to enter an OID: Begin with "." and separate by ".". For example, .3.4.5.2
Mask	Specifies the mask values of the filter. You can enter a two-digit value only.
Type	Specifies if you want to include or exclude an IP address entry from the address list of the MIB tables.
<b>SNMPv3 &gt; Target Parameter tab</b>	
Target Parameter Name	Specifies the target parameter name that is used while sending a trap to a target. A security device can support up to 32 target parameters.
Filter	Specifies the filter that you have created. Each filter is tagged to a target (host).
Security Model	Specifies the security model of the target parameter.
Security Level	Specifies the security level of the target parameter.
Community	Specifies the community that you have created.
<b>SNMPv3 &gt; Target Address tab</b>	
Target Name	Specifies the target name.
IPv4/IPv6 Address	Specifies either the IPv4 or IPv6 IP address. The system sends the trap to the target if the mask is 32 for IPv4 addresses or 128 for IPv6 addresses.
Netmask/Prefix	Specifies the netmask of the IPv4 or IPv6 IP address.
Port	Specifies the port.
Target Parameter	Specifies the target parameter that you have created.
Tag List	Specifies the tag value that you have selected in the filter.

- Related Documentation**
- [General Report Settings for ScreenOS Devices Overview on page 166](#)
  - [Device Administration Options for ScreenOS Devices Overview on page 146](#)





## CHAPTER 6

# Security

Before configuring security, you must first enable and set up the Profiler. 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. For details on analyzing your network, see the *Network and Security Manager Administration Guide*. This chapter provides information on setting up the Profiler and configuring antivirus settings, including antispam and Web filtering.

This chapter contains the following topics:

- [Classification of Security Options Overview on page 174](#)
- [Classification of Antivirus Scanning Overview on page 174](#)
- [External Antivirus Scanner Settings Overview on page 175](#)
- [Internal Antivirus Scan Manager Settings Overview on page 176](#)
- [Internal Antivirus HTTP Webmail Settings Overview on page 179](#)
- [Antivirus Scanner Settings Overview on page 179](#)
- [Classification of Deep Inspection Methods on page 181](#)
- [Attack Object Database Overview on page 182](#)
- [Using Attack Objects Overview on page 183](#)
- [Antispam Settings in ScreenOS Overview on page 184](#)
- [Configuring Antispam Settings in ScreenOS \(NSM Procedure\) on page 185](#)
- [Configuring IDP Security Module Settings in ScreenOS Overview on page 187](#)
- [Configuring Integrated Web Filtering in ScreenOS \(NSM Procedure\) on page 188](#)
- [Example: Configuring Integrated Web Filtering \(NSM Procedure\) on page 188](#)
- [Redirect Web Filtering in ScreenOS Using NSM Overview on page 190](#)

- [Example: Configuring Redirect Web Filtering in ScreenOS \(NSM Procedure\) on page 191](#)
- [Adding Proxy Addresses Overview on page 192](#)

---

## Classification of Security Options Overview

The security screen contains security options that you can set for the device. In the Device dialog box, open the Security heading to see configuration options. For instructions for configuring specific device settings, see the *Network and Security Manager Online Help*.

This topic describes the following security options:

- Antivirus settings
- Deep inspection
- Attack database
- Attack objects
- Antispam
- IDP SM settings
- Web filtering

### Related Documentation

- [Classification of Antivirus Scanning Overview on page 174](#)
- [External Antivirus Scanner Settings Overview on page 175](#)
- [Internal Antivirus Scan Manager Settings Overview on page 176](#)

---

## Classification of Antivirus Scanning Overview

A virus is executable code that infects or attaches itself to other executable code to reproduce itself. Some malicious viruses erase files or lock up systems, while other viruses merely infect files and can overwhelm the target host or network with bogus data.

Juniper Networks supports internal and external antivirus (AV) scanning on select security devices. Use the antivirus (AV) option to configure AV scanning. Security devices may provide one or more of the following antivirus scanning methods:

- External AV scanning—Uses an external Trend Micro device for scanning. (Supported in ScreenOS 5.2. Not supported in ScreenOS 5.3 or later.) The security device forwards all traffic to be scanned to the Trend Micro device. To configure external AV scanning, use the AV Scanner settings.
- Internal AV scanning—Uses the AV scanner on the security device and is not supported by all security devices. To configure internal AV scanning, use the AV Scan Manager settings (see [“Internal Antivirus Scan Manager Settings Overview” on page 176](#)).
- Internet Content Adaptation Protocol (ICAP) scanning—Uses an external ICAP server or server group for scanning. Supported in ScreenOS 5.4 and later. Use the ICAP object and ICAP AV object in Object Manager to create ICAP AV objects. These objects are

not assigned to the security device. Instead, they are assigned through a Rule option in a security policy. See [“DNS Server Configuration Using DNS Settings” on page 103](#).

You can also configure the internal AV scanner to scan webmail responses from a Web server to a client. For information, see [“Internal Antivirus HTTP Webmail Settings Overview” on page 179](#).

The various antivirus scan settings are as follows:

- External Antivirus Scanner Settings
- Internal Antivirus Scan Manager Settings
- Internal Antivirus HTTP Webmail Settings
- Antivirus Scanner Settings

**Related Documentation**

- [External Antivirus Scanner Settings Overview on page 175](#)
- [Internal Antivirus Scan Manager Settings Overview on page 176](#)
- [Classification of Security Options Overview on page 174](#)

## External Antivirus Scanner Settings Overview

You can use the AV Scanner Settings tab to configure the AV scanner options available in the UI. [Table 40 on page 175](#) describes the AV Scanner Settings tab options.

**Table 40: External AV Scanner Settings**

External AV Scanner Options	Description
Maximum Number of TCP connections	The maximum number of connections between the security device and the external AV scanner.
Fail Mode Traffic Permit	When enabled, the security device continues to permit traffic even if the device loses connectivity with the AV scanner.
Fail Mode Scanner Threshold	The number of times the security device consecutively fails to make contact with the external scanner before going into a 5-minute wait period. After the wait period, the security device again attempts to reach the external scanner.
Maximum AV resources allowed per AV client	The maximum percentage of AV resources that an AV client can consume. The default is 70%; the acceptable range is from 1 to 100%, where 100% allows unrestricted resource consumption. You might want to edit this option to prevent a malicious user from generating a large amount of traffic in an attempt to consume all available resources.

Table 40: External AV Scanner Settings (*continued*)

External AV Scanner Options	Description
HTTP Settings	<ul style="list-style-type: none"> <li>• HTTP keep-alive—This option directs the device to use the HTTP keep-alive connection option. Using this option prevents the device from sending a TCP FIN message to indicate termination of data transmission.</li> <li>• Skip scanning HTTP content with predefined content type—By default this option is enabled. This means HTTP scanning does not scan HTTP entities composed of any of the following Multipurpose Internet Mail Extensions (MIME) content types (and when followed by a slash, subtypes): <ul style="list-style-type: none"> <li>• application/x-director</li> <li>• application/pdf; image</li> <li>• video</li> <li>• audio</li> <li>• text/css</li> <li>• text/html</li> </ul> </li> </ul> <p>Because most HTTP entities are composed of these content types, HTTP scanning only applies to a small subset of HTTP entities such as /zip and application /exe content types, where viruses are most likely to be hiding.</p>
Trickling	You can direct the device to forward specific amounts of unscanned traffic to the HTTP client to prevent the client from timing out while the scanner is busy examining downloaded HTTP files. If you select <b>Custom</b> , you can specify the amounts that are forwarded. Selecting <b>Default</b> resets the amounts to their default values.

- Related Documentation**
- [Internal Antivirus Scan Manager Settings Overview on page 176](#)
  - [Internal Antivirus HTTP Webmail Settings Overview on page 179](#)
  - [Classification of Antivirus Scanning Overview on page 174](#)

## Internal Antivirus Scan Manager Settings Overview

You can use the AV Scan Manager Settings tab to configure the AV scanner options available in the UI. [Table 41 on page 176](#) describes the internal AV Scan Manager setting options.

Table 41: Internal AV Scan Manager Settings

Internal AV Scan Manager Options	Your Action	Comments
Pattern Server URL	You specify the URL address of the server from which the device retrieves pattern file updates.	<p>You can use one of the following two default pattern-update URLs:</p> <ul style="list-style-type: none"> <li>• To use the Kaspersky internal antivirus scanner, <a href="http://update.juniper-updates.net/av/5gt">http://update.juniper-updates.net/av/5gt</a>.</li> <li>• To use the Trend Micro internal antivirus scanner, <a href="http://5gt-pactiveupdate.trendmicro.com/activeupdate/server.ini">http://5gt-pactiveupdate.trendmicro.com/activeupdate/server.ini</a>.</li> </ul>

Table 41: Internal AV Scan Manager Settings (*continued*)

Internal AV Scan Manager Options	Your Action	Comments
Update AV pattern through proxy	You can update AV patterns from a proxy server.	This update does not require Internet access and is done offline. You cannot configure an HTTPS proxy, because you cannot cache an HTTPS proxy.
Update Interval	You can specify the interval at which the device starts an automatic pattern update.	<b>NOTE:</b> You can direct a security device to immediately contact the pattern server and update its pattern file. To do this, right-click the device object and select <b>AV Scan Manager &gt; Update Pattern</b> . (You can modify the pattern server URL and update the interface if necessary.) Click <b>OK</b> .
Maximum Decompression level	You can specify the number of levels of compression to examine.	A setting of 2 will examine a compressed file within a compressed file. If the number of levels of compression in the file exceeds the number indicated here, the e-mail will be blocked.
Content drop parameters	You can specify that the device drop messages if the size of the content or the number of concurrent messages exceed configurable limits.	NA

Table 41: Internal AV Scan Manager Settings (*continued*)

Internal AV Scan Manager Options	Your Action	Comments
Content Protocol	You can select the type of protocols (HTTP, SMTP, FTP, IMAP or POP3) that are to be examined for virus patterns.	<p>For each protocol, you can also specify the following (not all values applicable to all protocols):</p> <ul style="list-style-type: none"> <li>• Scan Mode— All, Intelligent, or by File Extension. If you select Scan by File Extension, you must populate the Ext List Include box.</li> <li>• Scanning Timeout—Scans that take longer than this period are not completed.</li> <li>• Decompress Layer—The number of levels of decompression to uncompress before scanning. Supported by ScreenOS 5.3 and later. For ScreenOS 5.2 and earlier, you must configure on an individual scanner basis.</li> <li>• Skip Mime (HTTP only)—If checked, causes the scanner to skip any mime types listed in the Mime List box. Supported by ScreenOS 5.3 and later. For ScreenOS 5.2 and earlier, you must configure on an individual scanner basis.</li> <li>• Ext List Include—A list of file extensions to examine for viruses. Extension lists are created under Object Manager &gt; AV Objects &gt; Extension Lists.</li> <li>• Ext List Exclude—A list of file extensions to not examine for viruses. Extension lists are created under Object Manager &gt; AV Objects &gt; Extension Lists.</li> <li>• Mime List (HTTP only)—The list of mime types to not scan. NSM ships with a default mime type list, or you can create your own under Object Manager &gt; AV Objects &gt; Custom Mime Lists.</li> <li>• Virus Notification with Protocol Code—FTP, HTTP, IMAP, POP3, and SMTP only. Notifies the client when a virus is detected. The AV scanner uses the default warning messages or user-defined warning messages, and their respective protocol codes to notify the client. You can select this feature under Object Manager &gt; AV Objects &gt; Virus Notification with Protocol Code.</li> <li>• Email Notify Virus Sender (IMAP, POP3, and SMTP only)—Notifies an email sender if a virus was found in the e-mail.</li> <li>• Email Notify Scan-Error Sender (IMAP, POP3, and SMTP only)—Notifies an email sender if the e-mail was dropped due to a scan error.</li> <li>• Email Notify Scan-Error Recipient (IMAP, POP3, and SMTP only)—Notifies an e-mail recipient if the e-mail was passed because of a scan error.</li> <li>• Send admin e-mail after virus pattern file updated—Notifies the administrator through e-mail of an updated pattern file. You can indicate whether you want the device to notify the administrator through e-mail when an updated pattern file is available.</li> </ul>

**Related Documentation**

- [Internal Antivirus HTTP Webmail Settings Overview on page 179](#)
- [Antivirus Scanner Settings Overview on page 179](#)

- [External Antivirus Scanner Settings Overview on page 175](#)

## Internal Antivirus HTTP Webmail Settings Overview

You can configure the internal AV scanner to scan Webmail responses from a Web server to a client. When a client makes an HTTP Webmail request, the security device can intercept the Web Server response, scan the response for viruses, and then forward to the client.

Because networks typically handle a large amount of HTTP traffic, you might want to enable scanning for Webmail only. When enabled, the internal AV scanner scans HTTP traffic for Webmail only (non-Webmail HTTP traffic is not scanned). When disabled, the device scans all HTTP traffic for viruses.

The internal AV scanner examines specific HTTP Webmail patterns only (many popular providers are predefined). To configure Webmail scanning, you must define the URL parameters:

- **URL Pattern**—Specifies a URL pattern identifying a certain type of Webmail to examine for virus patterns. When the URL matches all of the following parameters, the AV scanner performs a virus scan.
- **Path in URL**—Specifies the download URL path for the Webmail.
- **Path Exclusion**—Excludes the listed path from scans. Supported in ScreenOS 5.3 and later.
- **Argument in URL**—Specifies the URL argument. Arguments begin with a question mark (?).
- **Argument Exclusion**—Excludes the listed argument from scans. Supported in ScreenOS 5.3 and later.
- **Host Name in URL**—Specifies the host name in the URL.
- **Host Exclusion**—Excludes the listed host from scans. Supported in ScreenOS 5.3 and later.

For more information about AV, refer to the *Concepts & Examples ScreenOS Reference Guide: Attack Detection and Defense Mechanisms*.

### Related Documentation

- [Antivirus Scanner Settings Overview on page 179](#)
- [Classification of Deep Inspection Methods on page 181](#)
- [Internal Antivirus Scan Manager Settings Overview on page 176](#)

## Antivirus Scanner Settings Overview

The third tab in the device-specific or template-specific antivirus settings is the AV Scanner Settings tab. [Table 42 on page 180](#) describes the antivirus scanner settings available:

Table 42: Antivirus Scanner Settings

Antivirus Scanner Options	Description
Fail Mode Traffic Permit	Select this check box if you want the device to forward unexamined traffic when it fails to contact the antivirus scanner. If you want the device to block unexamined traffic, leave the box clear.
Maximum AV resources allowed per AV client	Set the maximum percentage of device resources a single source can occupy at one time. Prevent one source from overwhelming the device.
HTTP keep alive	Select this check box to keep the HTTP connection alive while antivirus scanning occurs.
Trickling	<p>Forward some HTTP traffic to the requesting client so the browser does not time out during the antivirus scan. The following are the trickling settings and its respective steps for configuration:</p> <ul style="list-style-type: none"> <li>• Disable — Disables HTTP trickling.</li> <li>• Default — Enables HTTP trickling using the stated predefined parameters. If content length is larger than 3 MB, trickle 500 bytes for every 1 MB sent for scanning.</li> <li>• Custom — Enables HTTP trickling using user-defined parameters.</li> </ul> <p>To configure trickling:</p> <ol style="list-style-type: none"> <li>1. In the Minimum length to start trickling (MB) box, select the minimum size (in megabytes) of an HTTP file to trigger trickling. Note that you must enter a valid integer value less than 4096.</li> <li>2. In the Trickle for every (MB) box, select the size (in megabytes) of a block of traffic to which the security device applies trickling.</li> <li>3. In the Trickle size box (Bytes) box, select the size (in bytes) of unscanned traffic that the security device forwards.</li> </ol>
Warning message for virus notification	For FTP, HTTP, IMAP, POP3, and SMTP only. Allows you to customize the warning message for virus notification. When a virus is detected, the AV scanner appends the customized warning message to the default message and the device sends the message to the client. If you do not set a customized message, the AV scanner sends only the default warning message.
Subject of virus notification e-mail	For IMAP, POP3, and SMTP only. Allows you to set a customized subject for virus notification e-mail. When the AV scanner sends an AV notification e-mail to the client on detecting a virus, the AV scanner uses the default e-mail subject, if you do not set the customized subject. You can configure the AV scanner to use a customized subject for the virus notification email.
Source address of notification e-mail	For IMAP, POP3, and SMTP only. Allows you to set a customized source address for virus notification e-mail. When the AV scanner sends an AV notification e-mail to the client on detecting a virus, by default, the AV scanner uses the IP address of the security device. You can configure the AV scanner to use a customized source address for the virus notification e-mail.
Charset of virus notification e-mail	For IMAP, POP3, and SMTP only. Allows you to enter the character set for the notification e-mail. If the notification e-mail includes Japanese or other double-byte characters, you can specify the character set to be used to display the notification e-mail. For example, if the virus notification e-mail includes Japanese characters, you can set the charset to <i>shift_jis</i> .



- Related Documentation**
- [Classification of Deep Inspection Methods on page 181](#)
  - [Attack Object Database Overview on page 182](#)
  - [Internal Antivirus HTTP Webmail Settings Overview on page 179](#)

## Classification of Deep Inspection Methods

The Deep Inspection (DI) option is only available on some security devices. DI is a mechanism for filtering permitted traffic. When you enable DI in a firewall rule, the device examines permitted traffic and takes action if the DI module in ScreenOS finds attack signatures or protocol anomalies.



**NOTE:** Deep inspection is only available on standalone devices. It cannot be used to disable attacks when the device is in a cluster.

The Juniper Networks Security team provides multiple DI signature packs for different security needs. Packs are covered by license keys. You must get a license key to enable a signature pack. Only one signature pack can exist for a given device.

Available signature packs are as follows:

- Server Protection Pack
- Client Protection Pack
- Worm Mitigation Pack
- Baseline (Default) Pack

Use the Deep Inspection configuration screens to modify the default settings defined in RFCs and RFC extensions for the following protocols listed in [Table 43 on page 181](#).



**NOTE:** You can also enable the validation of all TCP packets for TCP checksum by selecting **Enable TCP Checksum**.

**Table 43: Deep Inspection: Supported Protocols**

Deep Inspection: Supported Protocols			
AIM	IDENT	NTP	SNMP/Trap
CHARGEN	IKE	POP3	SQL Mon
DHCP	IMAP	PortMapper	SSH
DISCARD	IRC	RADIUS	SSL
DNS	LDAP	Rexec	Syslog

Table 43: Deep Inspection: Supported Protocols (*continued*)

Deep Inspection: Supported Protocols			
ECHO	LPR	rlogin	TELNET
FINGER	MSN	SunRPC	TFTP
FTP	MSRPC	Rsh	VNC
GNUTELLA	MS-SQL	RTSP	WHOIS
GOPHER	NBNAME	Rusers	Yahoo Messenger
HTTP	NFS	SMB	
ICMP	NNTOP	SMTP	

For details on each protocol and its settings, refer to the **di** command in the *NetScreen CLI Reference Guide*.

For more information about DI, refer to the *Concepts & Examples ScreenOS Reference Guide: Attack Detection and Defense Mechanisms*.

**Related  
Documentation**

- [Attack Object Database Overview on page 182](#)
- [Using Attack Objects Overview on page 183](#)
- [Antivirus Scanner Settings Overview on page 179](#)

## Attack Object Database Overview

The Attack Object option is only available on some security devices. Use the Attack Database option to configure a database that contains all the predefined attack objects, organized into attack object groups by protocol and severity level.

Juniper Networks stores the attack object database on the attack object update server at <https://services.netscreen.com/restricted/sigupdates>. To gain access to the attack object update server, you must first obtain an attack object update subscription for your security device.

After you have obtained a subscription, you must update the attack object database on the GUI server and managed device. The update process differs slightly between devices running ScreenOS 5.1 and later and devices running 5.0; for details, see the “Managing Devices” section of the *Network and Security Manager Administration Guide*.

For all devices, the attack object database on the managed device must match the version of the attack object database on the GUI server. If the databases do not match, a validation icon appears next to the Attack Database Version setting, and the Disable Attack option does not appear in the device navigation tree.

To use the predefined attack objects, create a DI Profile object that references specific attack object groups and configure a firewall rule to use that profile object.

To configure the attack object database:

- Specify the URL of the attack object database server. NSM downloads the latest version of the attack object database from <https://services.netscreen.com/restricted/sigupdates>.
  - When you update the attack object database for a device running ScreenOS 5.0.x or later, the device connects to this URL and downloads the latest database version.
  - When you update the attack object database for a device running ScreenOS 5.1 and later, the management system automatically connects to the URL specified in the UI Preferences and downloads the new database version to the GUI server. ScreenOS 5.1 and later devices do not contact the Attack Object Database server URL directly.
  - You can update the DI patterns from a proxy server (ScreenOS 6.2 devices or later). This update does not require Internet connectivity and is done offline. You cannot configure an HTTPs proxy, because you cannot cache an HTTPs proxy. You can update the DI patterns only if you have disabled the deep inspection package selection.
- Specify the mode for checking and updating the database (ScreenOS 5.0 devices only):
  - Notification—Checks the attack object update server at specified times and notifies you if the database on the server is more recent than the database on the security device.
  - Update—Checks the attack object update server at specified times and automatically updates the database on the device if the database on the attack object update server is more recent.
- Specify the schedule (daily, weekly, or monthly) on which the security device checks the attack object update server.

You can also direct a security device to update its attack object database immediately, either from the attack object update server (ScreenOS 5.0 devices) or the NSM GUI server (ScreenOS 5.1 and later devices). For more information, see the “Managing Devices” section of the *Network and Security Manager Administration Guide*.

#### Related Documentation

- [Using Attack Objects Overview on page 183](#)
- [Antispam Settings in ScreenOS Overview on page 184](#)
- [Classification of Deep Inspection Methods on page 181](#)

## Using Attack Objects Overview

Occasionally, an attack object produces false positives when included in a security policy for your network. You can remove the attack from the firewall rule by removing the attack object group to which the attack belongs or by disabling the individual attack object at

the device level. Although disabling attack objects does not improve throughput performance for the security device, this fine-tuning of the attacks detected by each device helps reduce false positives in your logs.

To disable attack objects, the attack object database on the managed device must match the version of the database on the GUI server. If the databases do not match, the Disable Attacks option does not appear in the device navigation tree, and a validation icon appears next to the Attack Database Version setting in **Security > Attack DB > Settings**.

To disable an attack object on a device, double-click the device to open the device configuration. In the device navigation tree, select **Security > Attack DB > Disable Attacks**, and then select the attack objects you want to disable.



**NOTE:** Disabled attack objects are device-specific. For example, disabling an attack object within the root system does not disable the attack object in any of its virtual systems, and disabling an attack object in one vsys does not affect that attack object in any other vsys.

---

For more information about the attack object database, see the “Attack Detection and Defense Mechanisms” volume in the *Concepts & Examples ScreenOS Reference Guide*.

**Related  
Documentation**

- [Antispam Settings in ScreenOS Overview on page 184](#)
- [Configuring Antispam Settings in ScreenOS \(NSM Procedure\) on page 185](#)
- [Attack Object Database Overview on page 182](#)

---

## Antispam Settings in ScreenOS Overview

---

Spam consists of unwanted e-mail messages, usually sent by commercial, malicious, or fraudulent entities. The antispam feature examines transmitted messages to identify spam. When the device detects a message deemed to be spam, it either drops the message or tags the message field with a preprogrammed string. This antispam feature is not meant to replace your antispam server, but to complement it. Configuring this command prevents an internal corporate e-mail server from receiving and distributing spams. Devices running ScreenOS 5.3 or later support antispam functionality.

You can configure antispam to tag or block unwanted e-mails based on e-mail ID, hostname, domain name, or IP address. SMTP is supported but not POP3 or IMAP. Advanced features such as Bayesian filtering are not supported.

E-mail is tagged or blocked based on blacklists and whitelists, which can be configured locally. Juniper Networks provides a server with a blacklist of known spammers. NSM first attempts to match each e-mail against the local lists. If it does not match a local list, it then attempts to match the e-mail against the list on the Juniper Networks server. [Table 44 on page 185](#) lists the match criteria for the local whitelist, local blacklist, Juniper Networks blacklist, and corresponding actions.

Table 44: Whitelist and Blacklist Criteria

Whitelist and Blacklist Criteria			
Match	Match	Not Checked	No Action (allow through)
Match	No Match	Not Checked	No Action (allow through)
No Match	Match	Not Checked	Block or Tag
No Match	No Match	Match	Block or Tag
No Match	No Match	No Match	No Action (allow through)

**Related Documentation**

- [Configuring Antispam Settings in ScreenOS \(NSM Procedure\) on page 185](#)
- [Configuring IDP Security Module Settings in ScreenOS Overview on page 187](#)
- [Using Attack Objects Overview on page 183](#)

## Configuring Antispam Settings in ScreenOS (NSM Procedure)

To configure a security device for antispam, you must turn on antispam in a policy and configure antispam settings on a device.

To configure antispam settings:

1. Double-click a security device in Device Manager.
2. Select **Security > Antispam**.
3. Populate the listed boxes:

- Antispam Whitelist—E-mails that contain e-mail addresses, IP addresses, hostnames, or domain names in this list will always be accepted by the filter, even if the e-mail also matches an entry in the blacklist.
  - Antispam Blacklist—E-mails that contain e-mail addresses, IP addresses, hostnames, and domain names in this list will be tagged or blocked, unless the e-mail also contains a match in the whitelist.
  - Action for Spam—Indicates whether email that matches a blacklist entry will be tagged and passed along or blocked.
  - Tag Subject or Header—If blacklist e-mails are to be tagged, indicates whether the tag will be placed in the header or subject line of the e-mail before it is passed on.
  - Tag String—If blacklist e-mails are to be tagged, indicates the character string that will be placed in the e-mail.
  - Enable use default SBL server—If checked, compare e-mails that do not match the local blacklist or whitelist to the blacklist of known spammers on the Juniper Networks server. If this check box is clear, only the local lists will be used.
4. Click **OK** to save the changes.

Install an antispam license key to enable the antispam option on the security device. For more information, see “Managing Devices” in the *Network and Security Manager Administration Guide*.

To check the status of the antispam option for a device:

1. Double-click the device configuration and select **Info > Capabilities**. If the license has been installed, Antispam Profiles is enabled.
2. Double-click the **my\_antispam\_policy** policy.
3. Double-click the Rule Options cell in the desired rule row.
4. Select the **Antispam** tab in the Configure Options dialog box.
5. Select the **Enable Antispam Profile** check box.
6. Select **ns-profile** from the Profile Name pull-down menu.
7. Click **OK** to close the Configure Options dialog box.

In the following example, you configure the device and put the string **\*\*\*SPAM\*\*\*** in the subject line of e-mails from wesendspam.com.

1. In the NSM navigation tree, select **Device Manager > Security Device > Templates**. Double-click a template to open it.
2. In the device navigation tree, select **Security > Antispam**.
3. Click the **Add** icon in the Antispam Blacklist area.
4. Enter **wesendspam.com** in the Entry box, and then click **OK**.
5. In the Action for Spam box, select **Tag Spam Email**.
6. In the Tag Subject or Header box, select **subject**.

7. In the Tag String box, enter **\*\*\*SPAM\*\*\***.
8. Select the **Enable use default SBL server** check box.
9. Click **OK** to save your changes to the template.

**Related  
Documentation**

- [Configuring IDP Security Module Settings in ScreenOS Overview on page 187](#)
- [Configuring Integrated Web Filtering in ScreenOS \(NSM Procedure\) on page 188](#)
- [Antispam Settings in ScreenOS Overview on page 184](#)

## Configuring IDP Security Module Settings in ScreenOS Overview

The IDP SM and sensor settings specify how the security module(s) on the ISG Series devices and IDP sensors handle traffic. When you add IDP, default values for all security module parameters are used. For more information, see the *Configuring Intrusion Detection and Prevention Devices Guide*.

This chapter includes the following topics:

- [Load-Time Parameters on page 187](#)
- [Run-Time Parameters on page 187](#)
- [Protocol Thresholds and Configuration on page 187](#)

### Load-Time Parameters

Load-time parameters include options for tuning IDP performance. In general, you modify these settings only if you encounter performance issues. These options control the security module functions when it first powers on. On devices running ScreenOS 6.3, you can make two CPUs share a policy. Eventually, the memory usage increases while the attacks database grows.

### Run-Time Parameters

Run-time parameters include options for tuning IDP detection methods. In general, you modify these settings only if you encounter false positives or performance issues. These options control the security module operations.

### Protocol Thresholds and Configuration

The protocol anomaly detection methods identify traffic that deviates from RFC specifications. In general, you modify protocol thresholds and configuration settings only if you encounter false positives or performance issues.

**Related  
Documentation**

- [Configuring Integrated Web Filtering in ScreenOS \(NSM Procedure\) on page 188](#)
- [Example: Configuring Integrated Web Filtering \(NSM Procedure\) on page 188](#)
- [Configuring Antispam Settings in ScreenOS \(NSM Procedure\) on page 185](#)

## Configuring Integrated Web Filtering in ScreenOS (NSM Procedure)

---

Web filtering enables you to manage Internet access by preventing access to inappropriate Web content. For more information on antispam and Web filtering, see the *Concepts & Examples ScreenOS Reference Guide*. Use the Web Filtering option to manage Internet access and prevent access to inappropriate Web content.

To configure a security device for Web filtering:

1. Install a Web license key to enable the Web Filtering option on the security device. For details, see “Managing Devices” section of the *Network and Security Manager Administration Guide*. To check the status of the Web Filtering option for a device, double-click the device configuration and select **Info > Capabilities**. If the license has been installed, Web filtering (Integrated) is enabled.
2. Configure at least one Domain Name Server (DNS) so the security device can resolve the SurfControl CPA server name to an address. For information about DNS, see “DNS Server Configuration Using DNS Settings” on page 103.
3. Select a Web filtering method and configure the Web filtering settings on the security device. You can select one of the following Web filtering methods for each security device:
  - Integrated Web Filtering (SurfControl CPA)—Block or permit access to a requested website by binding a SurfControl-defined or custom Web filtering profile to a firewall rule for the security device. A Web filtering profile contains Web categories (list of predefined or custom URLs) and the action the security device takes (permit or block) when it receives a request to access a URL.
  - Redirect Web Filtering (SurfControl SCFP)—Block or permit access to different web sites based on SurfControl-defined URLs, domain names, and IP addresses.
  - Redirect Web Filtering (Websense)—Block or permit access to different websites based on Websense-defined URLs, domain names, and IP addresses.

Optionally, you can define categories and profiles. You can also assign a Web filtering profile to a firewall rule. For information, see the *Network and Security Manager Administration Guide*.

### Related Documentation

- [Example: Configuring Integrated Web Filtering \(NSM Procedure\) on page 188](#)
- [Redirect Web Filtering in ScreenOS Using NSM Overview on page 190](#)
- [Configuring IDP Security Module Settings in ScreenOS Overview on page 187](#)

## Example: Configuring Integrated Web Filtering (NSM Procedure)

---

With integrated Web filtering, you can permit or block access to a requested website by binding a Web Filtering profile to a firewall rule. A Web Filtering profile contains Web Categories and the action the security device takes (permit or block) when it receives a request to access a URL.



A Web category is a list of URLs organized by content. SurfControl Content Portal Authority (CPA) servers maintain a large database of all types of Web content classified into 40 categories. For a list of SurfControl Web Categories, see “Appendix C, SurfControl Web categories,” in the *Network and Security Manager Administration Guide*.

SurfControl has three server locations that each serve a specific geographic area: the Americas, Asia Pacific, and Europe/Middle East/Africa. The default primary server is the Americas; the default backup server is Asia Pacific.

URLs and categories created and maintained by SurfControl appear in the NSM UI as predefined, and cannot be edited. You can also create custom URLs, and then use those URLs within a custom Web Filtering Profile.

In this example, you select SurfControl CPA (Integrated) as your Web Filtering profile.

To configure integrated Web filtering:

1. In the NSM navigation tree, select **Device Manager > Devices**, and then double-click the device for which you want to configure Web Filtering. The device configuration appears.
2. In the device navigation tree, select **Security > Web Filtering**, and then click the **SurfControl CPA (Integrated)** tab.
3. Select **CPA Server Enable**, and then configure the following SurfControl Settings:
  - For Server, select **America**.
  - For Primary Host, enter **usi.SurfCA.com**.
  - For Primary Port, enter **9020**.
  - For Fail Mode select **block**.
  - Select **Enable Cache**, and then configure the following cache settings:
    - For Cache Timeout (hours), enter **24**.
    - For Cache Size (K bytes), enter **500**.
    - For Query Interval (weeks), enter **2**.
  - Select **Enable Group-based URL Filtering**, and then configure the following group-based URL filtering options:
    - For User Group select **juniper**.
    - For Priority select **1**.
    - For Bound Profile select **ns-profile (predefined)**.
  - Click **OK** to save your settings and close the device configuration.

#### Related Documentation

- [Redirect Web Filtering in ScreenOS Using NSM Overview on page 190](#)
- [Configuring Integrated Web Filtering in ScreenOS \(NSM Procedure\) on page 188](#)

- Example: Configuring Redirect Web Filtering in ScreenOS (NSM Procedure) on page 191

## Redirect Web Filtering in ScreenOS Using NSM Overview

Redirect Web Filtering enables you to block or permit access to different websites based on their URLs, domain names, and IP addresses. NSM supports redirect Web filtering using either the Websense Enterprise Engine or SurfControl Web Filter.



**NOTE:** For Websense licensing information, go to [www.websense.com](http://www.websense.com). For SurfControl licensing information, go to [www.surfcontrol.com](http://www.surfcontrol.com).

For Websense, ScreenOS supports up to eight Web-filtering servers. On vsys devices, one server is reserved for the root, leaving seven servers available for vsys (one server per vsys, all remaining vsys must use the root server). For vsys-capable devices running ScreenOS 5.2, you can assign the same server to multiple vsys devices, and then configure a profile name for each vsys to enable the filtering server to distinguish between vsys devices.

Select the redirect Web filtering method you want to use, enable Web filtering for that method, and then configure the settings.

Table 45 on page 190 describes the options available for configuring Web filtering settings.

**Table 45: Web Filtering Options**

Web Filtering Options	Description
Source Interface	The source from which the security device initiates Web filter requests to a Web-filtering server.
Server Name	The IP address or fully qualified domain name (FQDN) of the Websense or SurfControl server.
Server Port	The port number on the filtering server that handles filtering requests. The default port for Websense is 15868; the default port for SurfControl is 15868.
Profile Name	<p>The profile name uniquely identifies the device when connecting to the filtering server. When configuring Websense (Redirect) Web-Filtering for multiple vsys devices using the same root device, you can assign the same Web-filtering server and port to multiple vsys devices as long as you use a unique profile name for each device.</p> <p><b>NOTE:</b> This option is applicable for vsys capable devices running ScreenOS 5.2 only.</p>
Server Timeout	The time interval, in seconds, that the security device waits for a response from the Web-filtering server. If the server does not respond within the time interval, the security device either blocks the request or permits it. For the time interval, you can enter a number between 10 and 240.
Fail Mode	The fail mode (Block or Permit) determines how the security device handles HTTP requests if the device loses contact with the Web-filtering server.

Table 45: Web Filtering Options (*continued*)

Web Filtering Options	Description
Message Type	<p>The source of the message the user receives when Websense or SurfControl blocks a site.</p> <ul style="list-style-type: none"> <li>If you select <b>NetPartners Websense/SurfControl</b>, the security device forwards the message it receives from the Websense or SurfControl server.</li> <li>If you select <b>NetScreen</b>, the security device sends the message that you entered in the Message Sent to Blocked Client box.</li> </ul>
Message Sent to Blocked Client	<p>The message the security device returns to the user after blocking a website. You can use the message sent from the Websense or SurfControl server, or create a message (up to 500 characters).</p>

If you change the default port on the server you must also change the port on the security device.

All vsys devices assigned to the same WebSense Web-Filtering server use the same Server Timeout, Fail Mode, and Message Type. Although you can configure different values for these fields for different vsys devices in the NSM UI, the WebSense server uses only the values defined for the vsys device that most recently contacted the Web-Filtering server.

If you select NSM, some of the functionality that Websense provides, such as redirection, is suppressed.

- Related Documentation**
- [Example: Configuring Redirect Web Filtering in ScreenOS \(NSM Procedure\) on page 191](#)
  - [Example: Configuring Integrated Web Filtering \(NSM Procedure\) on page 188](#)
  - [Configuring Integrated Web Filtering in ScreenOS \(NSM Procedure\) on page 188](#)

### Example: Configuring Redirect Web Filtering in ScreenOS (NSM Procedure)

Select **Websense (Redirect)** as your Web filtering policy. The following example explains how to configure redirect Web filtering in ScreenOS devices.

To configure redirect Web filtering in ScreenOS devices:

1. In the NSM navigation tree, select **Device Manager > Devices**, and then double-click the device for which you want to configure Web filtering. The device configuration appears.
2. In the device navigation tree, select **Security > Web Filtering**, and then click the **Websense (Redirect)** tab.
3. Select **Enable Web Filtering**, and then configure the following WebSense settings:

- For Source Interface, select **untrust**.
- For Server Name, enter **10.1.2.5**.
- For Server Port, enter **15868**.
- For Server Timeout (in seconds), enter **10**.
- For Fail Mode, select **Permit**.
- For Message Type, select **NetScreen**.
- For Message Sent to Blocked Client, enter **We're sorry, but the requested URL is prohibited. Contact ntwksec@mycompany.com**.
- Click **OK** to save your settings and close the device configuration.

**Related  
Documentation**

- [Adding Proxy Addresses Overview on page 192](#)
- [Redirect Web Filtering in ScreenOS Using NSM Overview on page 190](#)

---

## Adding Proxy Addresses Overview

---

For ScreenOS 6.1 or later, you can add the proxy address value for http and ssl as pattern updates. You can create the proxy value under **Device Manager > Devices > Security > Proxy**.

**Related  
Documentation**

- [Example: Configuring Redirect Web Filtering in ScreenOS \(NSM Procedure\) on page 191](#)
- [Redirect Web Filtering in ScreenOS Using NSM Overview on page 190](#)

## CHAPTER 7

# Planning and Preparing VPNs

Planning and preparing VPN components includes the following topics:

- [System-Level and Device-Level VPN Using NSM Overview on page 194](#)
- [System-Level VPN with VPN Manager Overview on page 194](#)
- [Device-Level VPN in Device Manager Overview on page 195](#)
- [VPN Configuration Supported Overview on page 196](#)
- [Planning Your VPN Using NSM Overview on page 196](#)
- [Defining VPN Members and Topology Using NSM on page 198](#)
- [Traffic Protection Using Tunneling Protocol in NSM Overview on page 200](#)
- [Traffic Protection Using IPsec Tunneling Protocol Overview on page 201](#)
- [Traffic Protection Using L2TP Tunneling Protocol Overview on page 203](#)
- [VPN Tunnel Types Overview on page 203](#)
- [Defining VPN Checklist Overview on page 205](#)
- [Defining Members and Topology in NSM on page 205](#)
- [Defining Traffic Types for Data Protection in NSM on page 205](#)
- [Defining VPN Traffic Using Security Protocols in NSM on page 206](#)
- [Defining Tunnel Creation Methods in NSM on page 206](#)
- [Preparing Basic VPN Components on page 208](#)
- [Preparing Required Policy-Based VPN Components Overview on page 209](#)
- [Policy-Based VPN Creation Using Address Objects and Protected Resources Overview on page 209](#)
- [Policy-Based VPN Creation Using Shared NAT Objects Overview on page 210](#)
- [Policy-Based VPN Creation Using Remote Access Server Users Overview on page 211](#)
- [Configuring Required Routing-Based VPN Components Overview on page 213](#)
- [Routing-Based VPN Support Using Tunnel Interfaces and Tunnel Zones Overview on page 213](#)
- [Routing-Based VPN Support Using Static and Dynamic Routes Overview on page 214](#)
- [Preparing Optional VPN Components Overview on page 214](#)

- [Optional VPN Support Using Authentication Servers Overview on page 215](#)
- [Optional VPN Support Using Certificate Objects Overview on page 215](#)

## System-Level and Device-Level VPN Using NSM Overview

With Network and Security Manager (NSM), 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.

NSM 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, and 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.

### Related Documentation

- [System-Level VPN with VPN Manager Overview on page 194](#)
- [Device-Level VPN in Device Manager Overview on page 195](#)
- [VPN Configuration Supported Overview on page 196](#)

## System-Level VPN with VPN Manager Overview

For AutoKey IKE and L2TP VPNs, create the VPN at the system level using VPN Manager. [Table 46 on page 194](#) describes the different VPNs that the VPN Manager supports.

**Table 46: VPNs Supported**

VPNs	Description
AutoKey IKE VPNs	Used 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	Connect and authenticate multiple L2TP remote access server (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, and then use these objects in multiple VPNs.

Table 46: VPNs Supported (*continued*)

VPNs	Description
Compact and Expanded Views	Choose the Compact (default) or Expanded view to create your VPN. Both views offer the same configuration options.
Autogenerated Tunnels	Create tunnel interfaces on each route-based VPN member automatically. Use the device tunnel summary to review all autogenerated tunnels in the VPN.
Autogenerated VPN Rules	Create all VPN rules with a single click. NSM 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, logging, limiting the number of sessions from each source IP towards servers to a given threshold count, and so on), and 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 NSM, you must create the VPN at the device level in Device Manager.

**Related  
Documentation**

- [System-Level and Device-Level VPN Using NSM Overview on page 194](#)
- [Device-Level VPN in Device Manager Overview on page 195](#)
- [VPN Configuration Supported Overview on page 196](#)

## Device-Level VPN in Device Manager Overview

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.

**Related  
Documentation**

- [VPN Configuration Supported Overview on page 196](#)
- [System-Level VPN with VPN Manager Overview on page 194](#)
- [Planning Your VPN Using NSM Overview on page 196](#)

## VPN Configuration Supported Overview

---

NSM supports all possible VPN configurations that are supported by the CLI and Juniper Networks ScreenOS Web UI, 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 server (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.

### Related Documentation

- [Planning Your VPN Using NSM Overview on page 196](#)
- [Device-Level VPN in Device Manager Overview on page 195](#)
- [Defining Members and Topology in NSM on page 205](#)

## Planning Your VPN Using NSM Overview

---

NSM 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 topics provide information to help you make these decisions.

- [Determining Your VPN Members and Topology](#)
- [Protecting Data in the VPN](#)
- [Choosing a VPN Tunnel Type](#)
- [VPN Checklist](#)

### Related Documentation

- [Defining Members and Topology in NSM on page 205](#)



- [Traffic Protection Using Tunneling Protocol in NSM Overview on page 200](#)
- [Traffic Protection Using IPsec Tunneling Protocol Overview on page 201](#)

## Defining VPN Members and Topology Using NSM

---

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 NSM, 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.

Table 47 on page 199 describes the various types of topologies.

**Table 47: VPN Types**

Topology	Description
Network Address Translation (NAT)	<p>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.</p> <p>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.</p>
Site-to-Site	<p>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.</p> <ul style="list-style-type: none"> <li>• Advantages—Simple, easy to configure.</li> <li>• Disadvantages—The central security device is a single point of failure.</li> </ul> <p>Use a site-to-site VPN to connect remote networks to a single, central network inexpensively. An example is shown below:</p>

Table 47: VPN Types (*continued*)

Topology	Description
Hub and Spoke	<p>In a hub and spoke VPN, multiple security devices (spokes) communicate through a central device (the hub).</p> <ul style="list-style-type: none"> <li>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.</li> <li>Disadvantages—The hub is a single point of failure; however, you can use NSRP for redundancy.</li> </ul> <p>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.</p> <p>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:</p>
Full Mesh	<p>In a full mesh VPN, all VPN member can communicate with all other VPN members.</p> <ul style="list-style-type: none"> <li>Advantages—Because a full mesh configuration uses redundant IPSec tunnels, traffic continues to flow even if a node fails.</li> <li>Disadvantages—When you add a member to the VPN, you must reconfigure all devices.</li> </ul> <p>Use a full mesh VPN when you need to ensure that every VPN member can communicate with every other VPN member.</p>
Creating Redundancy	<p>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.</p>

- Related Documentation**
- [Traffic Protection Using Tunneling Protocol in NSM Overview on page 200](#)
  - [Traffic Protection Using IPsec Tunneling Protocol Overview on page 201](#)
  - [Planning Your VPN Using NSM Overview on page 196](#)

## Traffic Protection Using Tunneling Protocol in NSM Overview

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. NSM provides two tunneling protocols such as IPsec and L2TP.

- Related Documentation**
- [Traffic Protection Using IPsec Tunneling Protocol Overview on page 201](#)
  - [Traffic Protection Using L2TP Tunneling Protocol Overview on page 203](#)
  - [Defining Members and Topology in NSM on page 205](#)

## Traffic Protection Using IPsec Tunneling Protocol Overview

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 NSM, 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.

NSM supports the following IPsec data protection services for VPNs:

- [Using Authentication on page 201](#)
- [Using Encapsulating Security Payload \(ESP\) on page 201](#)

### Using Authentication

To authenticate the data in the VPN tunnel, you can use the AH protocol, preshared secrets, or certificates. [Table 48 on page 201](#) describes the data authentication in the VPN tunnel.

**Table 48: Data Authentication**

Authentication Types	Description
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), Secure Hash Algorithm-2 (SHA-2), or Hash-based Message Authentication Code (HMAC).
Preshared Secret	NSM generates an ephemeral secret, distributes the secret to each VPN node, and 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.

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. [Table 49 on page 202](#) describes how to configure keys.

**Table 49: Configuring Keys**

Generating Keys	Description
Manual Key IKE	You can 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	<p>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.</p> <p>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.</p> <p>IKE negotiations include two phases:</p> <ul style="list-style-type: none"> <li>• In Phase 1, two members establish a secure and authenticated communication channel.</li> <li>• In Phase 2, two members negotiate Security Associations for services (such as IPsec) that require key material and/or parameters.</li> </ul> <p>VPN nodes must use the same authentication and encryption algorithms to establish communication.</p>
Replay protection	In a replay attack, an attacker intercepts a series of legitimate packets and uses them to create a denial of service (DoS) against the packet destination or to gain entry to trusted networks. Replay protection enables your security devices to inspect every IPsec packet to see if the packet has been received before—if packets arrive outside a specified sequence range, the security device rejects them.

- Related Documentation**
- [Defining Members and Topology in NSM on page 205](#)
  - [Traffic Protection Using Tunneling Protocol in NSM Overview on page 200](#)

- [VPN Tunnel Types Overview on page 203](#)

## Traffic Protection Using L2TP Tunneling Protocol Overview

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 (For example, authenticate ADSL services using PPP for users with an ISP at the opposite side of a Telco IP/ATM network)
- Transmit non-IP protocols (For example, bridge Novell and other network protocols)

PPP can send IP datagrams over a serial link, and it is often used to enable dial-up users to connect to their ISP and to the Internet. PPP authenticates username and password, and assigns parameters such as IP address, IP gateway, and DNS. PPP can also tunnel non-IP traffic across a serial link, such as Novell IPX or Appletalk.

PPP is also useful because it can carry non-IP traffic and authenticate connections to RADIUS servers. However, because PPP is not an IP protocol, Internet routers and switches cannot route PPP packets. To route PPP packets, you use L2TP, which encapsulates PPP packet inside an Internet routable, UDP packet. L2TP VPNs support remote access service users using Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP) authentication.

### Using L2TP over AutoKey IKE

L2TP only transmits packets; for encryption, authentication, or other data protection services, you must further encapsulate the L2TP packet using AutoKey IKE.

#### Related Documentation

- [VPN Tunnel Types Overview on page 203](#)
- [Defining VPN Checklist Overview on page 205](#)
- [Traffic Protection Using IPsec Tunneling Protocol Overview on page 201](#)

## VPN Tunnel Types Overview

You can configure three types of VPN tunnels with NSM:

- Policy-based VPNs—The VPN tunnel is created and maintained only during the transfer of network traffic that matches a VPN rule, and it 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—Policy-based VPNs are connected 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 on page 204](#)
- [About Route-Based VPNs on page 204](#)

## 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 NSM to configure a policy based on the network components you want to protect, including protected resources, and 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 server (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.

### Related Documentation

- [Defining VPN Checklist Overview on page 205](#)
- [Defining Members and Topology in NSM on page 205](#)
- [Traffic Protection Using L2TP Tunneling Protocol Overview on page 203](#)



## Defining VPN Checklist Overview

---

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.

### Related Documentation

- [Defining Members and Topology in NSM on page 205](#)
- [Defining Traffic Types for Data Protection in NSM on page 205](#)
- [VPN Tunnel Types Overview on page 203](#)

## Defining Members and Topology in NSM

---

The different NSM members that you can connect to VPN are as follows:

- Devices
- Network components or protected resources
- Remote access server (RAS) users
- Extranet devices

The different methods of connecting the VPN members are as follows:

- 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.

### Related Documentation

- [Defining Traffic Types for Data Protection in NSM on page 205](#)
- [Defining VPN Traffic Using Security Protocols in NSM on page 206](#)
- [Defining VPN Checklist Overview on page 205](#)

## Defining Traffic Types for Data Protection in NSM

---

You can use the following traffic types for data protection:

- 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.

- Related Documentation**
- [Defining VPN Traffic Using Security Protocols in NSM on page 206](#)
  - [Defining Tunnel Creation Methods in NSM on page 206](#)
  - [Defining Members and Topology in NSM on page 205](#)

---

## Defining VPN Traffic Using Security Protocols in NSM

You can use the following keys 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.

- Related Documentation**
- [Defining Tunnel Creation Methods in NSM on page 206](#)
  - [Preparing Basic VPN Components on page 208](#)
  - [Defining Traffic Types for Data Protection in NSM on page 205](#)

---

## Defining Tunnel Creation Methods in NSM

You can use different ways to create the tunnel. They are:

- [Using VPN Manager on page 206](#)
- [Creating Device-Level VPNs on page 207](#)

### Using VPN Manager

When adding a VPN using the VPN Manager, you enter the VPN members, gateways, IKE properties, and VPN topology, and 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.

You can choose the VPN type that best matches your VPN requirements. [Table 50 on page 207](#) describes the VPN types that match your VPN requirements.

Table 50: VPN Types

VPN Types	Description
Autokey IKE VPN	<p>Use to authenticate and encrypt traffic between devices and/or protected resources. An Autokey IKE VPN supports:</p> <ul style="list-style-type: none"> <li>• Mixed-mode VPNs (policy-based members and route-based members)</li> <li>• Policy-based VPNs</li> <li>• Route-based VPNs</li> <li>• ESP and AH Authentication</li> <li>• ESP AutoKey IKE Encryption</li> <li>• IP traffic</li> <li>• Tunnels between devices (routing-based) and protected resources (policy-based)</li> </ul>
Autokey IKE RAS VPN	<p>Use to authenticate and encrypt traffic between remote users and protected resources. An Autokey IKE RAS VPN supports:</p> <ul style="list-style-type: none"> <li>• Policy-based VPNs</li> <li>• ESP and AH Authentication</li> <li>• ESP AutoKey IKE Encryption</li> <li>• IP traffic</li> <li>• Remote access users</li> </ul>
L2TP RAS VPN	<p>Use to authenticate (but not encrypt) PPP or other non-IP traffic between RAS users and protected resources. An L2TP RAS VPN supports:</p> <ul style="list-style-type: none"> <li>• Policy-based VPNs</li> <li>• AH Authentication</li> <li>• PPP or other non-IP traffic</li> <li>• Remote access users</li> </ul>
L2TP over Autokey IKE RAS VPN	<p>Use to authenticate and encrypt PPP traffic between remote users and protected resources. An L2TP over Autokey IKE RAS VPN supports:</p> <ul style="list-style-type: none"> <li>• Policy-based VPNs</li> <li>• ESP and AH Authentication</li> <li>• ESP AutoKey IKE Encryption</li> <li>• PPP or other non-IP traffic</li> <li>• Remote access users</li> </ul>

## Creating Device-Level VPNs

You can create the following VPN types:

- AutoKey IKE VPN
- Manual key IKE VPN
- L2TP VPN
- Redundant site-site VPN

- Related Documentation**
- [Preparing Basic VPN Components on page 208](#)
  - [Preparing Required Policy-Based VPN Components Overview on page 209](#)
  - [Defining VPN Traffic Using Security Protocols in NSM on page 206](#)

---

## Preparing Basic VPN Components

---

After you have determines 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 *Network and Security Manager Online Help*.

---

To create any type of VPN, ensure that all security devices you want to use in the VPN are managed by NSM and configured correctly.

- **Devices**—Add the security devices you want to include in the VPN to NSM, 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, and then add the extranet device to the VPN. 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, and then add the extranet device to the VPN.
- **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 “[Configuring Zones and Zone Properties in ScreenOS Devices Overview](#)” on page 39.

- Related Documentation**
- [Preparing Required Policy-Based VPN Components Overview on page 209](#)
  - [Policy-Based VPN Creation Using Address Objects and Protected Resources Overview on page 209](#)

- [Defining Tunnel Creation Methods in NSM on page 206](#)

## [Preparing Required Policy-Based VPN Components Overview](#)

---

A policy-based VPN requires several components:

- Address objects
- Protected resources
- NAT objects
- User objects

### **Related Documentation**

- [Policy-Based VPN Creation Using Address Objects and Protected Resources Overview on page 209](#)
- [Policy-Based VPN Creation Using Shared NAT Objects Overview on page 210](#)
- [Preparing Basic VPN Components on page 208](#)

## [Policy-Based VPN Creation Using Address Objects and Protected Resources Overview](#)

---

The policy-based VPN creation methods are as follows:

- [Configuring Address Objects on page 209](#)
- [Configuring Protected Resources on page 209](#)

### [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 the *Network and Security Manager Administration Guide*.

### [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, NSM removes the previous security device from all affected VPNs and adds the new security device. However, NSM 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 the *Network and Security Manager Administration Guide*.

**Related  
Documentation**

- [Policy-Based VPN Creation Using Shared NAT Objects Overview on page 210](#)
- [Policy-Based VPN Creation Using Remote Access Server Users Overview on page 211](#)
- [Preparing Required Policy-Based VPN Components Overview on page 209](#)

---

## Policy-Based VPN Creation Using Shared NAT Objects Overview

---

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 the *Network and Security Manager Administration Guide*.

**Related  
Documentation**

- [Policy-Based VPN Creation Using Remote Access Server Users Overview on page 211](#)
- [Configuring Required Routing-Based VPN Components Overview on page 213](#)
- [Policy-Based VPN Creation Using Address Objects and Protected Resources Overview on page 209](#)

## Policy-Based VPN Creation Using Remote Access Server Users Overview

For VPNs that support RAS users, you must create a user object to represent each user. NSM 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.

The topic includes:

- [Authenticating RAS Users on page 211](#)
- [Configuring Group IKE IDS on page 212](#)

### Authenticating RAS Users

You can authenticate or encrypt a RAS user using one or more of the following protocols. [Table 51 on page 211](#) describes the various protocols:

**Table 51: Authenticating RAS Users**

Protocols	Description
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 NSM uses to identify and authenticate the user during IKE Phase I negotiations. To simplify RAS management for large numbers of AutoKey IKE users, you can also create AutoKey IKE groups that use a shared group IKE ID.
L2TP	Uses Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP) for authentication (password sent in the clear).
Manual Key IKE	Uses IPsec ESP and AH for encryption and authentication. Because manual key users are device-specific, you create them in the security device configuration, not in the Object Manager. For details on creating manual key users, see <a href="#">“L2TP and Xauth Local Users Configuration Overview” on page 244</a> .

We strongly recommend that you do not use null AH with ESP.

NSM allows certificate with DC in certificate DN to be used for dial-up 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 D; for example, "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 elements: CN, OU, O, L, ST, C, E-mail.

NSM 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).

NSM devices authenticate a RAS IKE user's ID if the values in the RAS IKE user's ASN1-DN identity fields exactly match the values in the group IKE user's ASN1-DN identity fields. The container ID type supports multiple entries for each identity field (for example, "ou=eng,ou=sw,ou=screensos"). 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.

NSM also supports DC in wildcard when using ASN1-DN to create IKE ID or a group of wildcard ID. NSM 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*.

### Related Documentation

- [Configuring Required Routing-Based VPN Components Overview on page 213](#)
- [Routing-Based VPN Support Using Tunnel Interfaces and Tunnel Zones Overview on page 213](#)
- [Policy-Based VPN Creation Using Shared NAT Objects Overview on page 210](#)



## Configuring Required Routing-Based VPN Components Overview

A route-based VPN requires two components:

- Tunnel interface or zone
- Route (static or dynamic)

For VPNs created with VPN Manager, you create the VPN first to autogenerate the tunnel interfaces, and 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.

### Related Documentation

- [Routing-Based VPN Support Using Tunnel Interfaces and Tunnel Zones Overview on page 213](#)
- [Routing-Based VPN Support Using Static and Dynamic Routes Overview on page 214](#)
- [Policy-Based VPN Creation Using Remote Access Server Users Overview on page 211](#)

## Routing-Based VPN Support Using Tunnel Interfaces and Tunnel Zones Overview

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 network address translation (NAT), use unnumbered interfaces.

- **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 “[Routing-Based VPN Support Using Tunnel Interfaces and Tunnel Zones Overview](#)” on page 213.

- Related Documentation**
- [Routing-Based VPN Support Using Static and Dynamic Routes Overview on page 214](#)
  - [Preparing Optional VPN Components Overview on page 214](#)
  - [Configuring Required Routing-Based VPN Components Overview on page 213](#)

---

## Routing-Based VPN Support Using Static and Dynamic Routes Overview

---

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 [“Virtual Router Configurations for Root and Vsys Overview” on page 248](#).

- Related Documentation**
- [Preparing Optional VPN Components Overview on page 214](#)
  - [Optional VPN Support Using Authentication Servers Overview on page 215](#)
  - [Routing-Based VPN Support Using Tunnel Interfaces and Tunnel Zones Overview on page 213](#)

---

## Preparing Optional VPN Components Overview

---

In any type of VPN, you can also use three optional components:

- Authentication server
- Certificate and certificate revocation list objects
- PKI defaults

After you have created the component, you can use it to create your VPN.

- Related Documentation**
- [Optional VPN Support Using Authentication Servers Overview on page 215](#)
  - [Optional VPN Support Using Certificate Objects Overview on page 215](#)

- [Routing-Based VPN Support Using Static and Dynamic Routes Overview on page 214](#)

---

## Optional VPN Support Using Authentication Servers Overview

---

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 “[Device Administrator Authentication Overview](#)” on page 147.

### Related Documentation

- [Optional VPN Support Using Certificate Objects Overview on page 215](#)
- [Preparing Optional VPN Components Overview on page 214](#)

---

## Optional VPN Support Using Certificate Objects Overview

---

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.

The following topics explain in more detail the optional VPN support using certificate objects:

- [Configuring Local Certificates on page 215](#)
- [Configuring CA Objects on page 216](#)
- [Configuring CRL Objects on page 216](#)

## 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 a independent

CA (or use your own internal CA, if available) to obtain a local device certificate file (a .cer file).

You must install this local certificate file on the managed device using NSM 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 [“Local Certificate Validation of ScreenOS Devices Overview” on page 266](#).

## 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, and then use this file to create a CA object.

You must install this CA certificate on the managed device using NSM before you can use the 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 the *Network and Security Manager Administration Guide*.

## 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, and then use this file to create a CRL object.

You must install the CRL on the managed device using NSM 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 the *Network and Security Manager Administration Guide*.

- Related Documentation**
- [Optional VPN Support Using Authentication Servers Overview on page 215](#)
  - [Preparing Optional VPN Components Overview on page 214](#)

## CHAPTER 8

# 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 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 *Network and Security Manager Online Help* Topic “VPNs” .

- [Device Level VPN Types and Supported Configurations Overview on page 219](#)
- [Device Level AutoKey IKE VPN: Using Gateway Configuration Overview on page 219](#)
- [Device Level AutoKey IKE VPN: Using Routes Configuration Overview on page 225](#)
- [Device-Level AutoKey IKE VPN: Using VPN Configuration Overview on page 225](#)
- [Device-Level AutoKey IKE VPN: Using VPN Rule Configuration Overview on page 228](#)
- [Device-Level Manual Key VPN: Using XAuth Users Overview on page 229](#)
- [Device-Level Manual Key VPN: Using Routing-Based VPN Overview on page 229](#)
- [Device-Level Manual Key VPN: Using VPN Configuration Overview on page 230](#)
- [Device Level Manual Key VPN: Using VPN Rule Configuration Overview on page 232](#)
- [Device Level L2TP VPN: Using L2TP Users Configuration Overview on page 233](#)
- [Device Level L2TP VPN: Using L2TP Configuration Overview on page 233](#)
- [Device Level L2TP VPN: Using VPN Rule Configuration Overview on page 234](#)

- [Creating Device Level L2TP-over-Autokey IKE VPNs Overview on page 235](#)
- [Adding VPN Rules to a Security Policy Overview on page 235](#)
- [Example: Creating Device Level VPN Type 1 \(NSM Procedure\) on page 236](#)
- [Example: Creating Device Level VPN Type 2 \(NSM Procedure\) on page 241](#)
- [Example: Creating Device Level VPN Type 3 \(NSM Procedure\) on page 242](#)
- [L2TP and Xauth Local Users Configuration Overview on page 244](#)
- [Configuring L2TP Local Users \(NSM Procedure\) on page 245](#)
- [XAuth Users Authentication Overview on page 247](#)
- [Vsys Configurations in NSM Overview on page 248](#)
- [Virtual Router Configurations for Root and Vsys Overview on page 248](#)
- [Zone Configurations for Root and Vsys Overview on page 249](#)
- [Interface Configurations for Root and Vsys Overview on page 251](#)
- [Viewing Root and Vsys Configurations on page 252](#)
- [Managing Inter-Vsys Traffic with Shared DMZ Zones on page 252](#)
- [Example: Routing Traffic to Vsys Using VLAN IDs \(NSM Procedure\) on page 252](#)
- [Example: Routing Traffic to Vsys Using IP Classification \(NSM Procedure\) on page 255](#)
- [Layer 2 Vsys Configuration Overview on page 257](#)
- [Assigning L2V VLAN IDs \(NSM Procedure\) on page 258](#)
- [L2V VLAN Groups in NSM Overview on page 258](#)
- [Predefined L2V Zones in NSM Overview on page 259](#)
- [L2V Interface Management in NSM Overview on page 260](#)
- [Converting L2V to VLAN Trunking \(NSM Procedure\) on page 261](#)
- [Configuring Crypto-Policy Overview on page 264](#)
- [Certificate Authentication Support in NSM Overview on page 265](#)
- [Self-Signed Certificates in NSM Overview on page 266](#)
- [Local Certificate Validation of ScreenOS Devices Overview on page 266](#)
- [Generating Certificate Requests to ScreenOS Devices \(NSM Procedure\) on page 267](#)
- [Loading Local Certificate into NSM Management System on page 269](#)
- [Installing Local Certificates Using SCEP in NSM on page 270](#)
- [Manual Installation of Local Certificates in NSM on page 270](#)
- [Certificate Authority Configuration in NSM Overview on page 271](#)
- [Installing CA Certificates Using SCEP in NSM on page 271](#)
- [Manual Installation of CA Certificates in NSM on page 272](#)
- [Configuring Certificate Revocation Lists \(NSM Procedure\) on page 273](#)
- [Imported Certificates in NSM Overview on page 273](#)
- [PKI Default Settings Configuration in NSM Overview on page 274](#)

## Device Level VPN Types and Supported Configurations Overview

You can create four types of device-level VPNs. [Table 52 on page 219](#) describes the types of device-level VPNs:

**Table 52: Device-Level VPN Types**

Device-Level VPN Types	Description
AutoKey IKE VPN	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 <a href="#">"Device Level AutoKey IKE VPN: Using Gateway Configuration Overview" on page 219</a> .
Manual Key IKE VPNs	Authenticate devices, protected resources, and RAS users in the VPN with manual keys. For details on each step, see <a href="#">"Device-Level Manual Key VPN: Using XAuth Users Overview" on page 229</a> .
L2TP RAS VPN	Connect L2TP RAS users and protected resources with authentication but without encryption. For details on each step, see <a href="#">"Device Level Manual Key VPN: Using VPN Rule Configuration Overview" on page 232</a> .
L2TP-over-AutoKey IKE RAS VPN	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 <a href="#">"Creating Device Level L2TP-over-Autokey IKE VPNs Overview" on page 235</a> .

Creating device-level AutoKey IKE VPNs is a four stage process:

### 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.

### Related Documentation

- [Device Level AutoKey IKE VPN: Using Gateway Configuration Overview on page 219](#)
- [Device Level AutoKey IKE VPN: Using Routes Configuration Overview on page 225](#)
- [Device-Level AutoKey IKE VPN: Using VPN Configuration Overview on page 225](#)

## Device Level AutoKey IKE VPN: Using Gateway Configuration Overview

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

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 topics.

- [ScreenOS Devices Gateway Properties on page 220](#)
- [ScreenOS Devices IKE IDs or XAuth Identification Number on page 222](#)
- [Security Methods for ScreenOS Devices on page 224](#)

## ScreenOS Devices Gateway Properties

Enter a name for the new gateway, and then specify the following gateway values as described in [Table 53 on page 220](#):

**Table 53: Gateway Properties**

Gateway Options	Description
Mode	<p>The mode determines how Phase 1 negotiations occur.</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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 <b>must</b> use Aggressive mode for VPNs that include RAS users.</li> </ul>



Table 53: Gateway Properties (*continued*)

Gateway Options	Description
Remote Gateway	<p>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. From ScreenOS 6.3, Remote Gateway supports IPv6.</p> <ul style="list-style-type: none"> <li>• Static IP Address—For remote gateways that use a static IP address, enter the IP address and mask.</li> <li>• RAS User/Group—For remote gateways that are users, select the user object or user group object that represents the RAS user.</li> <li>• Dynamic IP Address—For remote gateways that use a dynamic IP address, select dynamic IP address.</li> </ul>
Authenticated by EAP	<p>This option provides IKEv2 EAP pass-through. You can enable a ScreenOS 6.1 device to use EAP to authenticate a client with a RADIUS authentication server. The device acts as a proxy (authenticator) and passes the EAP messages between the client (supplicant) and the RADIUS (authentication) server.</p> <p>During EAP exchanges, the device decapsulates the EAP messages in IKEv2 messages from the peer, encapsulates them into RADIUS messages, and sends them to the RADIUS server. When the RADIUS server responds to the authentication requests, the device decapsulates the EAP messages, encapsulates them into IKEv2 messages, and sends them to the peer. After the RADIUS server has authenticated the client, if there is a shared secret generated during the exchange, the security device extracts the shared secret from the RADIUS Access-Accept message and uses it to generate the AUTH payload. In this way, the device passes the EAP messages between a client and an authentication server.</p>
Outgoing Interface	<p>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.</p>
Heartbeats	<p>Heartbeats are used to enable redundant gateways. You can use the default or set your own thresholds:</p> <ul style="list-style-type: none"> <li>• Hello—Enter the number of seconds the security device waits between sending hello pulses.</li> <li>• Reconnect—Enter the maximum number of seconds the security device waits for a reply to the hello pulse.</li> <li>• Threshold—Enter the number of seconds that the security device waits before attempting to reconnect.</li> </ul>
Dead Peer Detection	<p>Dead Peer Detection (DPD) is a protocol used by network devices to verify the current existence and availability of other peer devices. You can use DPD as an alternative to the IKE heartbeat but you cannot use both features simultaneously. You can configure the following DPD parameters:</p> <ul style="list-style-type: none"> <li>• Interval(Seconds) — Specifies the DPD interval. This interval is the time (in seconds) that the device allows to pass before considering a peer to be dead.</li> <li>• Always Send Switch — Instructs the device to send DPD requests regardless of whether there is IPsec traffic with the peer or not.</li> <li>• Retry Times — Specifies the maximum number of times to send the response request before considering the peer to be dead.</li> <li>• Reconnect(Seconds) — Specifies the reconnect interval. The parameter renegotiates the tunnel at configured intervals after it is cleaned up because of a dead peer detected.</li> </ul>

Table 53: Gateway Properties (*continued*)

Gateway Options	Description
NAT Traversal	<p>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-T for remote users that must connect to the VPN over an external NAT device.</p> <p>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.</p> <p>To use NAT-T, enable NAT-T and specify:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• Keepalive 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.</li> </ul>
Auth-Method	<p>The authentication method specified for this proposal. When the user does not specify the authentication method in the proposal, preshared key authentication will be used as the default authentication method. This is in line with the behavior of IKEv2.</p> <ul style="list-style-type: none"> <li>• Authentication method for this device—Select any of the authentication method you want to use. You can use certificates or preshared objects. With certificates, IKE uses a trusted authority defined in your network for the certificate server. You must define this trusted certificate authority by creating a certificate authority object. With preshared secrets, IKE generates an ephemeral secret and propagates it to each VPN node. This is secure because it propagates only within the VPN.</li> <li>• Peer's authentication type—Both phases use proposals when they negotiate a connection. Both peers must use the same authentication and encryption algorithms to establish communication.</li> </ul>

In ScreenOS 6.1 or later, NSM allows users to configure IKEv2. The remote gateway type for IKEv2 can be an interface with either a static IP address type or a RAS type.

## ScreenOS Devices IKE IDs or XAuth Identification Number

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. [Table 54 on page 223](#) describes the different ID type for each member.

Table 54: IKE IDs/XAuth Types

ID Types	Description
ASN1-DN	<p>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.</p> <ul style="list-style-type: none"> <li>At the peer ID, specify values for the Container Match and Wildcard Match.</li> <li>At the local ID, specify the value.</li> </ul> <p>Using a group ID can make configuring and maintaining your VPN quicker and easier. For details on how group IKE IDs work, see, <a href="#">Configuring Group IKE IDs</a> section in "<a href="#">Policy-Based VPN Creation Using Remote Access Server Users Overview</a>" on page 211. For details on determining the ASN1-DN container and wildcard values for group IKE IDs, see the <i>Juniper Networks ScreenOS 5.x Concepts and Examples Guide</i>.</p>
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; for example, <a href="#">server1.colorado.mycompany.com</a> .
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 e-mail address, such as <a href="#">user1@mycompany.com</a> .
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	<p>Use to specify the authentication server that assigns TCP/IP settings to the remote gateway.</p> <ul style="list-style-type: none"> <li>XAuth Server Name—Select a preconfigured authentication server object. For details on creating authentication server objects, see "<a href="#">Device Administrator Authentication Overview</a>" on page 147.</li> <li>Allowed Authentication Type—Select generic or Challenge Handshake Authentication Protocol (CHAP) (password is sent in the clear) to authenticate the remote gateway.</li> <li>Query Remote Setting—Enable this option to query the remote settings object for DNS and WINS information.</li> <li>Users and Groups—Authenticate XAuth RAS users using the authentication server, by enabling User or User Group and selecting a preconfigured user object.</li> </ul>
XAuth Client	<p>Use when the remote gateway is a RAS user that you want to authenticate.</p> <ul style="list-style-type: none"> <li>Allowed Authentication Type—Select <b>Any</b> or <b>Challenge Handshake Authentication Protocol (CHAP)</b> for authentication (password is sent in the clear).</li> <li>User Name and Password—Enter the username and password that the RAS user must provide for authentication.</li> </ul> <p><b>NOTE:</b> All passwords handled by NSM are case-sensitive.</p>
Bypass Authentication	Use to permit VPN traffic from this VPN member to pass unauthenticated by the Auth server.

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.

## Security Methods for ScreenOS Devices

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, and then click **Generate Key**. NSM 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 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” in the *Network and Security Manager Administration Guide*.

If your VPN includes only security devices, you can specify one predefined or custom proposal that NSM propagates to all nodes in the VPN. If your VPN includes extranet devices, you should use multiple proposals to increase security and ensure compatibility.

In ScreenOS 6.1 or later, the user can set the following IKEv2 parameters:

- Half opened IKE session threshold for triggering stateless cookie exchange.
- Initiator sending dummy IPsec packet.

- [IKE SA softlifetime.](#)

**Related Documentation**

- [Device Level AutoKey IKE VPN: Using Routes Configuration Overview on page 225](#)
- [Device-Level AutoKey IKE VPN: Using VPN Configuration Overview on page 225](#)
- [Device Level VPN Types and Supported Configurations Overview on page 219](#)

---

## Device Level AutoKey IKE VPN: Using Routes Configuration Overview

For a routing-based VPN member, you must configure:

- Tunnel zone or tunnel interfaces on the member.
- Static or dynamic routes from the member to other VPN members.

VPN traffic flows through the tunnel zones or tunnel interfaces on the security device, and uses static or dynamic routes to reach other VPN members. You must create the tunnel zones and interfaces before configuring routes.

For details on configuring tunnel zones, tunnel interfaces, static routes, or dynamic routes, see [“Configuring Virtual Routers” on page 292](#).

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.

**Related Documentation**

- [Device-Level AutoKey IKE VPN: Using VPN Configuration Overview on page 225](#)
- [Device-Level AutoKey IKE VPN: Using VPN Rule Configuration Overview on page 228](#)
- [Device Level AutoKey IKE VPN: Using Gateway Configuration Overview on page 219](#)

---

## Device-Level AutoKey IKE VPN: Using VPN Configuration Overview

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 NSM 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.

The following topics explain how to configure device-level autokey IKE VPN using VPN configuration:

- [Device-Level AutoKey IKE VPN Properties on page 226](#)
- [ScreenOS Security Measures Using VPN Configuration on page 226](#)
- [Binding/ProxyID on page 227](#)
- [Monitor Management on ScreenOS Devices Using AutoKey IKE VPN on page 228](#)

## Device-Level AutoKey IKE VPN Properties

Enter the following values as described in [Table 55 on page 226](#).

**Table 55: Device-Level AutoKey IKE VPN Properties**

Properties	Your Action
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	<p>Configure the mode:</p> <ul style="list-style-type: none"> <li>Use tunnel mode for IPsec—Before an IP packet enters the VPN tunnel, NSM 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. The DSCP mark (which allows the user to configure the DSCP value for each route based VPN) supports only Tunnel IPsec mode.</li> <li>Use transport mode for L2TP-over-IPsec—NSM 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.</li> </ul>
Do not set Fragment Bit in the Outer Header	<p>The Fragment Bit controls how the IP packet is fragmented when traveling across networks.</p> <ul style="list-style-type: none"> <li>Clear—Use this option to enable IP packets to be fragmented.</li> <li>Set—Use this option to ensure that IP packets are not fragmented.</li> <li>Copy—Select to use the same option as specified in the internal IP header of the original packet.</li> </ul>

## ScreenOS Security Measures Using VPN Configuration

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” in the *Network and Security Manager Administration Guide*.

If your VPN includes only security devices, you can specify one predefined or custom proposal that NSM 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 [“Routing-Based VPN Support Using Tunnel Interfaces and Tunnel Zones Overview” on page 213](#) and [“Configuring a Tunnel Interface” on page 87](#).

[Table 56 on page 227](#) describes the binding methods in the device.

**Table 56: Binding/ProxyID**

Binding Methods	Description
None	Select none when you do not want to bind the VPN tunnel to a tunnel interface or zone.
Tunnel Interface	Select a preconfigured 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. The user can set DSCP marking as a system for tagging traffic at a position within a hierarchy of priority.
Tunnel Zone	Select a preconfigured 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.
DSCP Marking	Select an option upon which the ScreenOS device overwrites the first 3 bits in the ToS byte with the IP precedence priority.
DSCP Value	Select the DSCP Value.
Proxy	<p>Select an option to define a proxy ID through either an IP address or an address name of the local and remote device.</p> <ul style="list-style-type: none"> <li>IP Address — Select this option to define multiple proxy IDs using an IP address. Upon selecting this option, you must set the new IP format settings.</li> <li>Address Book — Select this option to define multiple proxy IDs using an address book. Upon selecting this option, you must set the new address format settings.</li> <li>Disable — Select this option to disable the proxy parameter settings.</li> </ul>
Proxy ID Check	Select this option to enable the proxy-ID check on a route-based VPN. From ScreenOS 6.3, proxy ID check supports IPv6.

You can also enable proxy and configure the proxy parameters. When multiple tunnels exist between peers, the security device cannot use the route to direct the traffic through a particular tunnel. In such cases, the security device uses multiple proxy IDs to direct the traffic. You can use either an IP address or an address name of the local and remote device to define a proxy ID.

## Monitor Management on ScreenOS Devices Using AutoKey IKE VPN

You can enable VPN Monitor and configure the monitoring parameters for the device. Monitoring is off by default. Select the **VPN Monitor in Realtime Monitor** to display statistics for the VPN tunnel as described in [Table 57 on page 228](#).

**Table 57: Monitor**

VPN Monitor Status	Description
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. From ScreenOS 6.3, VPN monitor supports IPv6.
Rekey	<p>When enabled, the device regenerates the IKE key after a failed VPN tunnel attempts to reestablish 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:</p> <ul style="list-style-type: none"> <li>• Keep the VPN tunnel up even when traffic is not passing through</li> <li>• Monitor devices at the remote site.</li> <li>• Enable dynamic routing protocols to learn routes at a remote site and transmit messages through the tunnel.</li> <li>• 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.</li> </ul>
Optimized	<p>This option appears only for devices running ScreenOS 5.x. When enabled, the device optimizes its VPN monitoring behavior as follows:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• Suppresses VPN monitoring pings when the tunnel passes both incoming and outgoing traffic. This can help reduce network traffic.</li> </ul>
Source Interface and Destination IP	These options configure VPN monitoring when the other end of the VPN tunnel is not a security device. Specify the source and destination IP addresses.

- Related Documentation**
- [Device-Level AutoKey IKE VPN: Using VPN Rule Configuration Overview on page 228](#)
  - [Device Level AutoKey IKE VPN: Using Routes Configuration Overview on page 225](#)

## Device-Level AutoKey IKE VPN: Using VPN Rule Configuration Overview

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 to a Security Policy Overview” on page 235](#).

**Related  
Documentation**

- [Device-Level Manual Key VPN: Using Routing-Based VPN Overview on page 229](#)
- [Device-Level AutoKey IKE VPN: Using VPN Configuration Overview on page 225](#)

---

## Device-Level Manual Key VPN: Using XAuth Users Overview

---

Creating a device-level Manual key VPN is a four stage process.

- Configure XAuth Users
- Configure Routes (Route-based only)
- Configure VPN on Device
- Add VPN rules to Security Policy

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, and 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.

**Related  
Documentation**

- [Device-Level Manual Key VPN: Using Routing-Based VPN Overview on page 229](#)
- [Device-Level AutoKey IKE VPN: Using VPN Configuration Overview on page 225](#)
- [Device-Level AutoKey IKE VPN: Using VPN Rule Configuration Overview on page 228](#)

---

## Device-Level Manual Key VPN: Using Routing-Based VPN Overview

---

For a routing-based VPN member, you must configure:

- Tunnel zone or tunnel interfaces on the member.
- Static or dynamic routes from the member to other VPN members.

VPN traffic flows through the tunnel zones or tunnel interfaces on the security device, and uses static or dynamic routes to reach other VPN members. You must create the tunnel zones and interfaces before configuring routes. For details on configuring tunnel zones, tunnel interfaces, and static or dynamic routes, see [“Configuring Virtual Routers” on page 292](#).

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.

**Related Documentation**

- [Device-Level AutoKey IKE VPN: Using VPN Configuration Overview on page 225](#)
- [Device Level Manual Key VPN: Using VPN Rule Configuration Overview on page 232](#)
- [Device-Level AutoKey IKE VPN: Using VPN Rule Configuration Overview on page 228](#)

## Device-Level Manual Key VPN: Using VPN Configuration Overview

The following topics explain how to configure device-level manual key VPN using VPN configuration:

- [Device-Level Manual Key VPN Properties on page 230](#)
- [Binding on page 231](#)
- [Monitor Management on ScreenOS Devices Using Manual Key VPN on page 231](#)

### Device-Level Manual Key VPN Properties

Enter the following values to configure device-level manual key using VPN configuration as described in [Table 58 on page 230](#).

**Table 58: Device-Level Manual Key VPN Properties**

Device-Level Manual Key VPN Properties	Your Action
VPN Name	Enter a name for the VPN.
Gateway	Enter a gateway for the VPN.
Local SPI	Specify the local Security Parameter Index. This option also supports IPv6.
Remote SPI	Specify the remote Security Parameter Index. This option also supports IPv6.
Outgoing Interface	Specify the outgoing interface, which 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	<p>Select the fragment bit to control how the IP packet is fragmented when traveling across networks.</p> <ul style="list-style-type: none"> <li>• Clear—Use this option to enable IP packets to be fragmented.</li> <li>• Set—Use this option to ensure that IP packets are not fragmented.</li> <li>• Copy—Select to use the same option as specified in the internal IP header of the original packet.</li> </ul>

Table 58: Device-Level Manual Key VPN Properties (*continued*)

Device-Level Manual Key VPN Properties	Your Action
IPsec Protocol	<p>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.</p> <ul style="list-style-type: none"> <li>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.</li> </ul> <p><b>NOTE:</b> All passwords handled by NSM are case-sensitive.</p> <ul style="list-style-type: none"> <li>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.</li> </ul>

## 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 [“Routing-Based VPN Support Using Tunnel Interfaces and Tunnel Zones Overview” on page 213](#) and [“Configuring a Tunnel Interface” on page 87](#).

- None—Select none when you do not want to bind the VPN tunnel to a tunnel interface or zone.
- Tunnel Interface—Select a preconfigured 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. The user is able to set the DSCP marking and DSCP value. The DSCP value ranges from 0 through 63.
- Tunnel Zone—Select a preconfigured 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 Management on ScreenOS Devices Using Manual Key VPN

You can enable VPN Monitor and configure the monitoring parameters for the device. Monitoring is off by default. Enable the VPN Monitor in RealTime Monitor to display statistics for the VPN tunnel as described in [Table 59 on page 232](#).

Table 59: Monitor

VPN Monitor Status	Description
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	<p>When enabled, the device regenerates the IKE key after a failed VPN tunnel attempts to reestablish 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:</p> <ul style="list-style-type: none"> <li>• Keep the VPN tunnel up even when traffic is not passing through</li> <li>• Monitor devices at the remote site.</li> <li>• Enable dynamic routing protocols to learn routes at a remote site and transmit messages through the tunnel.</li> <li>• 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.</li> </ul>
Optimized	<p>This option appears only for devices running ScreenOS 5.x. When enabled, the device optimizes its VPN monitoring behavior as follows:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• Suppresses VPN monitoring pings when the tunnel passes both incoming and outgoing traffic. This can help reduce network traffic.</li> </ul>
Source Interface and Destination IP	When configured, these options use VPN Monitoring when the other end of the VPN tunnel is not a security device. Specify the source and destination IP addresses.

**Related Documentation**

- [Device Level Manual Key VPN: Using VPN Rule Configuration Overview on page 232](#)
- [Device Level L2TP VPN: Using L2TP Users Configuration Overview on page 233](#)
- [Device-Level Manual Key VPN: Using Routing-Based VPN Overview on page 229](#)

## Device Level Manual Key VPN: Using VPN Rule Configuration Overview

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 to a Security Policy Overview” on page 235](#).

- Related Documentation**
- [Device Level L2TP VPN: Using L2TP Users Configuration Overview on page 233](#)
  - [Device Level L2TP VPN: Using L2TP Configuration Overview on page 233](#)
  - [Device-Level Manual Key VPN: Using VPN Configuration Overview on page 230](#)

## Device Level L2TP VPN: Using L2TP Users Configuration Overview

Creating device-level L2TP VPN is a three stage process.

- Add L2TP Users
- Configure L2TP Settings
- Add VPN rules to Security Policy

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, and 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.

- Related Documentation**
- [Device Level L2TP VPN: Using L2TP Configuration Overview on page 233](#)
  - [Device Level L2TP VPN: Using VPN Rule Configuration Overview on page 234](#)
  - [Device Level Manual Key VPN: Using VPN Rule Configuration Overview on page 232](#)

## Device Level L2TP VPN: Using L2TP Configuration Overview

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, and then specify the following information as described in [Table 60 on page 233](#).

**Table 60: Device Level L2TP VPN: using L2TP Configuration**

L2TP Options	Description
Host Name	Enter the name of the L2TP host.

Table 60: Device Level L2TP VPN: using L2TP Configuration (*continued*)

L2TP Options	Description
Outgoing Interface	Specify the outgoing interface, which is the interface on the security device that sends and receives VPN traffic. Typically, the outgoing interface is in the untrust zone.
Keep Alive	Specify 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	<ul style="list-style-type: none"> <li>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 the <i>Network and Security Manager Administration Guide</i>.</li> <li>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.</li> </ul>

**Related Documentation**

- [Device Level L2TP VPN: Using VPN Rule Configuration Overview on page 234](#)
- [Creating Device Level L2TP-over-Autokey IKE VPNs Overview on page 235](#)
- [Device Level L2TP VPN: Using L2TP Users Configuration Overview on page 233](#)

## Device Level L2TP VPN: Using VPN Rule Configuration Overview

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 to a Security Policy Overview” on page 235](#).

**Related Documentation**

- [Creating Device Level L2TP-over-Autokey IKE VPNs Overview on page 235](#)
- [Adding VPN Rules to a Security Policy Overview on page 235](#)
- [Device Level L2TP VPN: Using L2TP Configuration Overview on page 233](#)

## Creating Device Level L2TP-over-Autokey IKE VPNs Overview

Creating a device-level L2TP-over-Autokey IKE VPN is a multi-stage process:

1. Add L2TP users (see [“Device Level L2TP VPN: Using L2TP Users Configuration Overview” on page 233](#))
2. Configure L2TP settings (see [“Device Level L2TP VPN: Using L2TP Configuration Overview” on page 233](#))
3. Configure peer gateway (see [“Device Level AutoKey IKE VPN: Using Gateway Configuration Overview” on page 219](#))
4. Configure routes (route-based only) (see [“Device Level AutoKey IKE VPN: Using Routes Configuration Overview” on page 225](#))
5. Add VPN to device (see [“Device-Level AutoKey IKE VPN: Using VPN Configuration Overview” on page 225](#))
6. Add VPN rules to security policy (see [“Device Level L2TP VPN: Using VPN Rule Configuration Overview” on page 234](#))

### Related Documentation

- [Adding VPN Rules to a Security Policy Overview on page 235](#)
- [Device Level L2TP VPN: Using VPN Rule Configuration Overview on page 234](#)

## Adding VPN Rules to a Security Policy Overview

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:

- [Configuring the VPN on page 235](#)
- [Configuring the Security Policy on page 236](#)
- [Assigning and Installing the Security Policy on page 236](#)

## Configuring the VPN

In security policies, select a predefined security policy (or create a 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—NSM 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 the *Network and Security Manager Administration Guide*.

To deny a host, use a deny rule before the VPN rule.

## Assigning and Installing the Security Policy

You must assign the security policy to each VPN member and install the security policy on those devices before the VPN is active.

### Related Documentation

- [Creating Device Level L2TP-over-Autokey IKE VPNs Overview on page 235](#)
- [Example: Creating Device Level VPN Type 1 \(NSM Procedure\) on page 236](#)
- [Example: Creating Device Level VPN Type 2 \(NSM Procedure\) on page 241](#)

---

## Example: Creating Device Level VPN Type 1 (NSM Procedure)

This topic provides examples of the two device-level VPN types with step-by-step instructions on creating each type of device-level VPN.



**NOTE:** For examples on creating other VPN types using VPN Manager, see the *Network and Security Manager Administration Guide*.

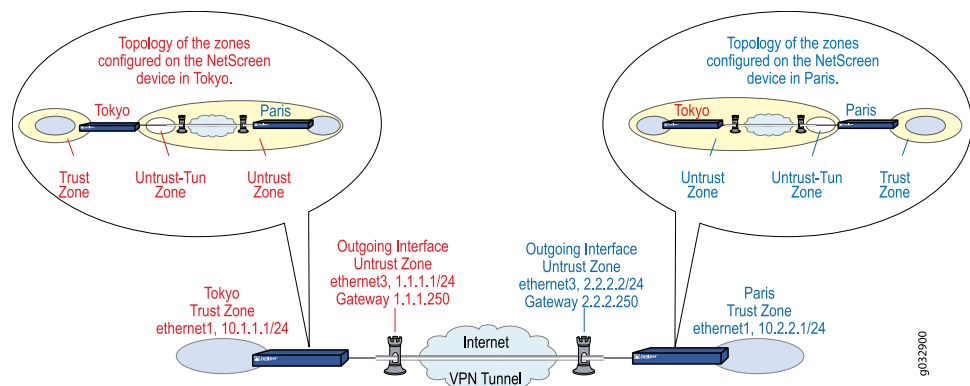
---



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 1: RB Site-to-Site VPN, MK Example Overview**



1. Add the Tokyo and Paris security devices (for details on adding devices, see “Adding Devices” in the *Network and Security Manager Administration Guide*). Begin by configuring 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.
2. 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.
3. Create the address objects that you use in the VPN rule in the firewall rulebase (for details on creating VPN rules, see the [“Adding VPN Rules to a Security Policy Overview” on page 235](#)).
4. 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 settings, and then click **OK**:
  - For Name, enter **Tokyo Trust LAN**.
  - For IP Address/Netmask, enter **10.1.1.0/24**.
  - Select **Use Wildcard Mask** if you want the wildcard mask to be sent as part of the address field instead of the Netmask.

- For Wildcard Mask, enter **10.1.1.0**.
  - For Color, select **magenta**.
  - For Comment, enter **Tokyo Trust Zone**.
5. 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 settings, and then click **OK**:
- For Name, enter **Paris Trust LAN**.
  - For IP Address/Netmask, enter **10.2.2.0/24**.
  - Select **Use Wildcard Mask** if you want the wildcard mask to be sent as part of the address field instead of the Netmask.
  - For Wildcard Mask, enter **10.2.2.0**.
  - For Color, select **magenta**.
  - For Comment, enter **Paris Trust Zone**.
6. Configure the Tokyo tunnel interface:
- In the NSM navigation tree, select **Device Manager > Devices**, and then double-click the Tokyo device to open the device configuration.
  - In the device navigation tree, select **Network > Interface**. Click the **Add** icon and select **Tunnel Interface**. The General Properties screen for tunnel.1 appears.
7. Configure the following settings, and then click **OK**:
- For Zone, select **untrust**.
  - For IP Options, select **Unnumbered**.
  - For Source Interface, select **ethernet3**.
8. Create the Tokyo VPN. In the device navigation tree, select **VPN Settings > AutoKey IKE/Manual VPN**.
9. Select the **Manual** tab, and then click the **Add** icon. The **Properties** screen appears. Configure the Properties tab as follows:
- For Name, enter **Tokyo\_Paris**.
  - For Gateway, enter **2.2.2.2**.
  - For Local SP, 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**, and then enter the password **asdlk24234**.
  - For Authentication Algorithm, select **SHA-1**.

- Select **Generate Key by Password**, and then enter the password **PNas134a**.
- Select the **Binding** tab. Select **Tunnel Interface**, and then select **tunnel.1**.

10. Click **OK** to save the new VPN.

11. Create Tokyo routes:

- 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.
- In the virtual router dialog box, click **Routing Table**, and then click the **Add** icon under destination-based routing table to add a new static route.



**NOTE:** ScreenOS 5.0.x devices display destination-based and source-based routing tables; ScreenOS 5.1 and later devices display destination-based, source-based, and source interface-based routing tables.

12. Configure a route from the untrust interface to the gateway, and then click **OK**.

13. Configure route from the trust zone to the tunnel interface, and then click **OK**.

14. Click **OK** to save your changes to the virtual router, and then click **OK** to save your changes to the Tokyo device.

15. Configure the Paris tunnel interface:

- In Device Manager, double-click the device icon for Paris to open the device configuration.
- In the device navigation tree, select **Network > Interface**. Click the **Add** icon and select **Tunnel Interface**. The General Properties screen appears.

16. Configure the following settings, and then click **OK**:

- For Zone, select **untrust**.
- For IP Options, select **Unnumbered**.
- For Source Interface, select **ethernet3**.

17. Create the Paris VPN:

- In the device navigation tree, select **VPN Settings > AutoKey IKE/Manual VPN**.
- Select the **Manual** tab, and then click the **Add** icon. The Properties screen appears.

18. Configure the following settings:

- For Name, enter **Paris\_Tokyo**.
- For Gateway, enter **2.2.2.2**.
- For Local SP, enter **3020**.
- For Remote SPI, enter **3030**.
- For Outgoing Interface, select **ethernet3**.

- For ESP/AH, select **ESP CBC**.
  - For Encryption Algorithm, select **3DES-CBC**, and then select **Generate Key by Password** and enter the password **asdlk24234**.
  - For Authentication Algorithm, select **SHA-1**, and then select **Generate Key by Password** and enter the password **PNas134a**.
19. Select the **Binding** tab. Select **Tunnel Interface**, and then select **tunnel.1**.
20. In the device navigation tree, select **Network > Virtual Router** to display the list of virtual routers on the device.
21. Click **OK** to save the new VPN.
22. Create Paris routes.
23. Double-click the trust-vr route to open the vr for editing.
24. In the virtual router dialog box, click **Routing Table**, and then click the **Add** icon under destination-based routing table to add a new static route.



**NOTE:** ScreenOS 5.0.x or later devices display both destination-based and source-based routing tables; ScreenOS 5.1 and later devices display destination-based, source-based, and source interface-based routing tables.

25. Configure a route from the untrust interface to the gateway, and then click **OK**.
26. Configure route from the trust zone to the tunnel interface, and then click **OK**.
27. Click **OK** to save your changes to the virtual router, and then click **OK** to save your changes to the Paris device.
28. Create the security policy:
- In the main navigation tree, select **Security Policies**. Click the **Add** icon to display the New Security Policy dialog box.
29. Configure the following settings, and then click **OK**:
- For Security Policy Name, enter **Corporate Route-based VPNs**.
  - Add comments, if desired.
30. In the NSM navigation tree, select **Security Policies > Corporate Route-based VPNs**. The security policy appears in the display area. Configure the rules.

**Related  
Documentation**

- [Example: Creating Device Level VPN Type 2 \(NSM Procedure\) on page 241](#)
- [Example: Creating Device Level VPN Type 3 \(NSM Procedure\) on page 242](#)
- [Adding VPN Rules to a Security Policy Overview on page 235](#)

## Example: Creating Device Level VPN Type 2 (NSM Procedure)

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.

1. Create VPN components:
  - Security devices.
  - Address objects.
2. Create the Tokyo VPN:
  - In the device navigation tree, select **VPN Settings > AutoKey IKE/Manual VPN**.
  - Select the **Manual** tab, and then click the **Add** icon. The Properties screen appears.
3. Configure the following settings:
  - For Name, enter **Tokyo\_Paris**.
  - For Gateway, enter **2.2.2.2**.
  - For Local SP, enter **3020**.
  - For Remote SPI, enter **3030**.
  - For Outgoing Interface, select **ethernet3**.
  - For ESP/AH, select **ESP CBC**.
  - For Encryption Algorithm, select **3DES-CBC**.
  - For Authentication Algorithm, select **SHA-1**.
4. Select **Generate Key by Password**, and then enter the password **PNas134a**.
5. Select the **Binding** tab. Select **Tunnel Zone** and select **untrust-tun**.
6. Click **OK** to save the new VPN.
7. Create Tokyo routes.
8. Create the Paris VPN:
  - In the device navigation tree, select **VPN Settings > AutoKey IKE/Manual VPN**.
  - Select the **Manual** tab, and then click the **Add** icon. The Properties screen appears.
9. Configure the following settings:

- For Name, enter **Paris\_Tokyo**.
  - For Gateway, enter **2.2.2.2**.
  - For Local SP, enter **3020**.
  - For Remote SPI, enter **3030**.
  - For Outgoing Interface, select **ethernet3**.
  - For ESP/AH, select **ESP CBC**.
  - For Encryption Algorithm, select **3DES-CBC**, and then select **Generate Key by Password** and enter the password **asdlk24234**.
  - For Authentication Algorithm, select **SHA-1**, and then select **Generate Key by Password** and enter the password **PNas134a**.
10. Select the **Binding** tab. Select **Tunnel Zoner** and select **untrust-tun**.
  11. Click **OK** to save the new VPN.
  12. Create Paris routes.
  13. Create the security policy:
    - In the NSM navigation tree, select **Security Policies**. Click the **Add** icon to display the new Security Policy dialog box.
  14. Configure the following settings, and then click **OK**:
    - For Security Policy Name, enter **Corporate Policy-Based VPN**.
    - Enter comments, if desired.
  15. In the NSM navigation tree, select **Security Policies > Corporate Policy-Based VPN**. The security policy appears in the display area. Configure two VPN rules as follows:
    - 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.
  16. Save the security policy.

**Related Documentation**

- [Example: Creating Device Level VPN Type 1 \(NSM Procedure\) on page 236](#)
- [Example: Creating Device Level VPN Type 3 \(NSM Procedure\) on page 242](#)
- [Adding VPN Rules to a Security Policy Overview on page 235](#)

---

### Example: Creating Device Level VPN Type 3 (NSM Procedure)

---

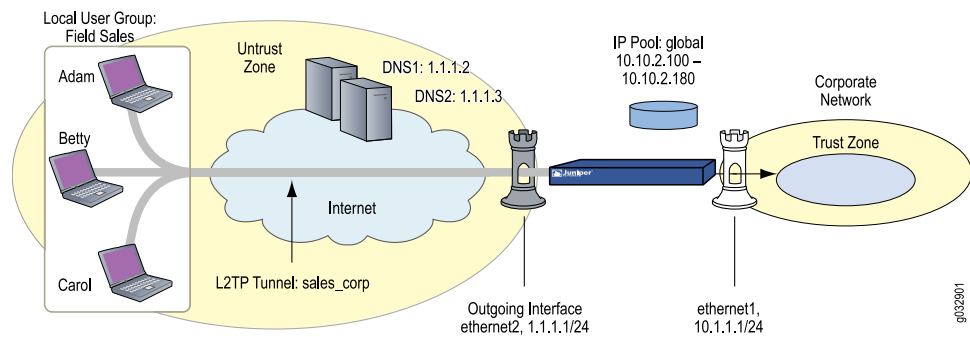
In this example, you create a RAS user group called Field Sales and configure an L2TP tunnel called Sales\_Corp, using ethernet3 (untrust zone) as the outgoing interface for the L2TP tunnel. The security device applies the default L2TP tunnel settings to the RAS user group.



**NOTE:** An L2TP-only configuration is insecure, and we only recommend it 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 as in Figure 2 on page 243.

**Figure 2: PB RAS VPN, L2TP Example Overview**



1. Configure the L2TP user objects. First, configure an L2TP user object for Adam, and then click **OK**:
  - For Name, enter **Adam**.
  - Select **Enable**, and then select **L2TP**.
  - Select **Password**, and then enter and confirm the password: **AJbioJ15**.
2. Configure an L2TP user object for Betty, and then click **OK**:
  - For Name, enter **Betty**.
  - Select **Enable**, and then select **L2TP**.
  - Select **Password**, and then enter and confirm the password: **BviPsoJ1**.
3. Configure an L2TP user object for Carol, and then click **OK**:
  - For Name, enter **Carol**.
  - Select **Enable**, and then select **L2TP**.
  - Select **Password**, and then enter and confirm the password: **Cs10kdD3**.
4. Create a local user group called Field Sales that includes the Adam, Betty, and Carol local user objects.
5. Configure the remote settings object. Configure the following settings, and 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 the *Network and Security Manager Administration Guide*.

6. Configure the IP pool object. Configure the following settings, and 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” in the *Network and Security Manager Administration Guide*.

7. Configure the L2TP tunnel:

- In Device Manager, double-click the device icon for the device on which you want to configure the L2TP tunnel.
- In the device navigation tree, select **VPN Settings > L2TP**. In the display area, click the **Add** icon. The null-L2TP tunnel dialog box appears.

8. Configure the following settings, and 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**, and then select **Field Sales**.

9. Click **OK** to save your changes to the device.

10. Configure a rule in the zone rulebase of a security policy.

**Related  
Documentation**

- [Example: Creating Device Level VPN Type 2 \(NSM Procedure\) on page 241](#)
- [Adding VPN Rules to a Security Policy Overview on page 235](#)

---

## L2TP and Xauth Local Users Configuration Overview

Use the L2TP/XAuth/Local User option to enable the security device to authenticate local users and/or assign specific IP pools and remote settings. Because user objects are



shared objects, you can configure the same user on multiple devices, but assign different remote settings and IP pool for each device.

You must configure a L2TP or XAuth local user on a security device when:

- You want the device to authenticate the user. Typically, you want to authenticate a user who is connecting to the device using a VPN tunnel.
- You want the device to assign specific IP, DNS server, and WINS server addresses to a user who is connecting to the device using a VPN tunnel. The remote settings and IP pool you assign at the device level override the remote settings and IP pool assigned to the VPN.

**Related  
Documentation**

- [Configuring L2TP Local Users \(NSM Procedure\) on page 245](#)
- [XAuth Users Authentication Overview on page 247](#)
- [Adding VPN Rules to a Security Policy Overview on page 235](#)

---

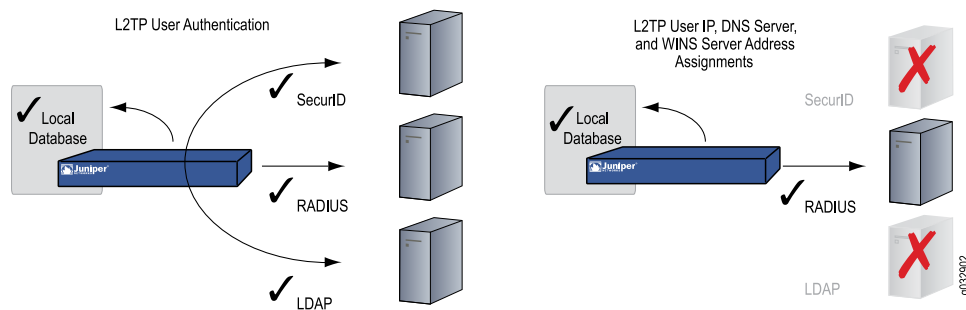
## Configuring L2TP Local Users (NSM Procedure)

The Layer 2 Tunneling Protocol (L2TP) enables a security device to authenticate users using the local database or an external auth server, and assign specific remote settings and IP pools.

L2TP enables the security device to authenticate users; to encrypt an L2TP VPN tunnel, you must apply an encryption scheme, such as IPsec, to the L2TP tunnel. When configuring an L2TP-over-IPsec VPN, you are actually setting up an L2TP tunnel and an IPsec tunnel with the same endpoints, and then linking the two tunnels together in a security policy rule. VPN Manager automatically generates the required rules; if you are creating the L2TP-over-IPsec VPN at the device-level, you must configure the rules manually. For more information about L2TP VPNs, see [“Device Level L2TP VPN: Using L2TP Users Configuration Overview” on page 233](#).

You can also use the device to assign specific IP, DNS server, and WINS server addresses from the local database or a RADIUS server. When you assign the L2TP user or user group a remote setting and IP pool at the device level, the settings override the remote settings and IP pool assigned to the VPN. You can even use different auth servers, one for each aspect of L2TP. For example, you might use a SecurID server to authenticate an L2TP user but make the address assignments from the local database.

Figure 3: Configure L2TP Local User



- In the NSM navigation tree, select **Object Manager > User Objects > Local Users**. In the display area, click the **Add** icon. Configure the following settings, and then click **OK**:

  - For Name, enter **Adam**.
  - For Color, select **orange**.
  - Select **Enable**, and then select **L2TP**.
  - Select **Password**, and then enter and confirm the password: **AJbioJ15**.

For information about how to create user objects, see the *Network and Security Manager Administration Guide*.
- In the NSM navigation tree, select **Object Manager > Remote Settings**. In the display area, click the **Add** icon. Configure the following settings, and then click **OK**:

  - For Name, enter **RM\_L2TP**.
  - For Color, select **green**.
  - Enter comments, if desired.
  - For Dns1, enter **1.1.1.2**.
  - For Dns2, enter **1.1.1.3**.
  - For Wins1, enter **0.0.0.0**.
  - For Wins2, enter **0.0.0.0**.

For information about how to create remote settings objects, see the *Network and Security Manager Administration Guide*.

  - In the NSM navigation tree, select **Object Manager > IP Pools**. Configure the new IP pool:
- In the display area, click the **Add** icon. The New IP Pool dialog box appears. Configure the following settings:

  - For IP Pool Name, enter **Global**.
  - For Color, select **magenta**.
  - Enter comments, if desired.

4. Click the **Add** icon. Configure the following settings and click **OK**:
  - For Start IP, enter **10.10.2.100**.
  - For End IP, enter **10.10.2.180**.
5. Click **OK** to save the new IP pool object. For information about how to create IP pool objects, see “Configuring IP Pools” in the *Network and Security Manager Administration Guide*.
6. Configure the L2TP local user:
  - In the NSM navigation tree, select **Device Manager > Devices**, and then double-click the device on which you want to configure the L2TP local user. The device configuration appears.
  - In the device navigation tree, select **L2TP/XAuth/Local User**, and then click the **Add** icon. The new L2TP/XAuth User Settings dialog box appears. Configure the following settings, and then click **OK**:
    - For User, select **Adam**.
    - For Remote Settings, select **RM\_L2TP**.
    - For IP Pool, select **Global**.
7. Click **OK** to save your changes to the device configuration.

**Related  
Documentation**

- [XAuth Users Authentication Overview on page 247](#)
- [L2TP and Xauth Local Users Configuration Overview on page 244](#)
- [Vsys Configurations in NSM Overview on page 248](#)

## XAuth Users Authentication Overview

The XAuth protocol enables the device to authenticate XAuth users and/or assign IP pools and remote settings.

An XAuth user (or user group) is a RAS user who authenticates when connecting to the security device using an AutoKey IKE VPN tunnel. Although both IKE and XAuth users can authenticate through an AutoKey IKE VPN tunnel, the authentication of IKE users is actually the authentication of VPN gateways or clients, while the authentication of XAuth users is the authentication of the individuals themselves. XAuth users must enter information that only they are supposed to know—their username and password.

You can also assign an XAuth user IP, WINS, and DNS addresses from the device. When you assign the XAuth user or user group a remote setting and IP pool at the device level, the settings override the remote settings and IP pool assigned to the VPN.

For more information about configuring authentication users on security devices, refer to the *Concepts & Examples ScreenOS Reference Guide: Fundamentals*.

**Related  
Documentation**

- [L2TP and Xauth Local Users Configuration Overview on page 244](#)

- [Vsys Configurations in NSM Overview on page 248](#)
- [Configuring L2TP Local Users \(NSM Procedure\) on page 245](#)

## Vsys Configurations in NSM Overview

---

A vsys is a virtual system that exists within a physical security device. By logically partitioning a single, physical security device into multiple virtual systems (each in its own domain), you can provide secure multitenant services. The physical device (known as the “root” device) shares some settings across all vsys, but each vsys also has its own unique settings. To enable the physical device to correctly route traffic to the appropriate vsys device, you must use VLAN tags at the vsys level or IP classification at the root level.

To add a vsys to the NSM system, you must first add a physical device that can contain vsys devices (NetScreen-500, 5000 line, ISG1000, and ISG2000 security devices support vsys), and then add each vsys to the physical device. An NSM administrator with full device configuration permissions can see both the root and vsys devices in a domain, but an administrator with only vsys permissions can see only the vsys devices in a domain. To create a secure, multi-tenant system, place the root device in the global domain and each vsys device in its own domain, and then assign vsys administrations to manage each domain. For details on adding a vsys, see “Adding Vsys Devices” in the *Network and Security Manager Administration Guide*.

After you have added or modeled a new root device and vsys to the NSM system, you must configure the vsys interfaces and subinterfaces, and any shared virtual routers and shared security zones on the root device. When importing an existing root device and vsys, NSM automatically imports the existing root and vsys settings from each device (physical and virtual).

The NetScreen 5000 line of security devices running ScreenOS 5.0 L2V also support vsys transparent mode, also known as Layer 2 vsys, or L2V vsys. To create an L2V vsys, when modeling the root device into NSM, ensure that the mode is set to Transparent (for imported devices, you must enable Transparent mode on the physical device using the Web UI or CLI).

For more information about vsys, refer to the *Concepts & Examples ScreenOS Reference Guide: Virtual Systems*. For more information about how to configure transparent vsys, refer to the *Juniper Networks New Features Guide* for ScreenOS 5.0-L2V software.

### Related Documentation

- [Virtual Router Configurations for Root and Vsys Overview on page 248](#)
- [Zone Configurations for Root and Vsys Overview on page 249](#)
- [XAuth Users Authentication Overview on page 247](#)

## Virtual Router Configurations for Root and Vsys Overview

---

At the root level, you can configure a virtual router as shareable, enabling that VR to be used by all vsys. By default, the untrust-vr is shared. To unshare a VR, you must remove all assigned vsys from a shared VR.

At the vsys level, you can configure the virtual routers as described in [Table 61 on page 249](#).

**Table 61: Virtual Router Configuration for Root and Vsys**

Virtual Routers	Description
Shared root-level virtual routers	By default, the root and vsys share the untrust-vr. However, you can configure a vsys to use any VR that is shared at the root-level.
Non-sharable vsys-level virtual router	This is a vsys-specific virtual router that, by default, maintains the routing table for the Trust- <i>vsysname</i> zone. By default, a vsys-level virtual router is named <i>vsysname-vr</i> (you can also customize the name to make it more meaningful). All vsys-level virtual routers are nonsharable.

- Related Documentation**
- [Zone Configurations for Root and Vsys Overview on page 249](#)
  - [Vsys Configurations in NSM Overview on page 248](#)
  - [Interface Configurations for Root and Vsys Overview on page 251](#)

## Zone Configurations for Root and Vsys Overview

At the root-level, you can configure a zone as shareable, enabling that zone to be used by all vsys. To share a zone, the zone must be in a shared virtual router; however, a shared virtual router can contain both shared and unshared zones.



**NOTE:** For details on configuring zones in L2V mode, see [“L2V VLAN Groups in NSM Overview” on page 258](#).

At the root level, all zones are available by default, as shown in [Table 62 on page 249](#).

**Table 62: Root-Level Zone Configuration**

Zone	Attribute	Description
Null	Shared	This zone is available by default.
Untrust	Shared	This zone is available by default.
Trust	Local	This zone is available by default.
DMZ	Local	This zone is available by default.
Self	Local	This zone is available by default.
MGT	Local	This zone is available by default.
HA	Local	This zone is available by default.
Global	Local	This zone is available by default.

**NOTE:**

- If an attribute for a root device is shared, the corresponding zone is inherited by all vsys devices that belong to the corresponding root device.
- All shared zones of the root device are inherited by all vsys devices that belong to the root device.
- If an attribute is local, corresponding zones are only applicable to corresponding root device.

At the vsys level, zones are automatically created or inherited as described in [Table 63 on page 250](#).

**Table 63: Vsys-Level Zone Configuration**

Zone	Attribute	Description
Trust-vsys_name	Local	This zone is created by default when you create the vsys.
Untrust-Tun-vsys_name	Local	This zone is created by default when you create the vsys.
Global-vsys_name	Local	This zone is created by default when you create the vsys.
Null	Shared	This zone is inherited from the root device.

**NOTE:**

- All shared zones of the root device are inherited by all vsys devices that belong to the root device.
- If an attribute is local, corresponding zones are only applicable to corresponding VSYS device.

Each vsys also supports user-defined security zones; you can bind these zones to any shared virtual routers defined at the root level or to the virtual router dedicated to that vsys.



**NOTE:** In ScreenOS 6.2, a new shared zone called shared-DMZ allows inter-vsys communications. NAT is also available for traffic from vsys-to-vsys based on the shared-DMZ zone to solve overlapping address issues. For details on configuring the shared DMZ zone, see the [“Managing Inter-Vsys Traffic with Shared DMZ Zones” on page 252](#).

- Related Documentation**
- [Interface Configurations for Root and Vsys Overview on page 251](#)
  - [Virtual Router Configurations for Root and Vsys Overview on page 248](#)
  - [Viewing Root and Vsys Configurations on page 252](#)

## Interface Configurations for Root and Vsys Overview

Interfaces can be dedicated, shared, imported, and exported between root and vsys.



**NOTE:** When the root system is in L2V, you cannot import or export interfaces. For more information, see [“Layer 2 Vsys Configuration Overview” on page 257](#).

At the root level, shared interfaces that are bound to a shared zone. However, any physical, subinterface, redundant interface, or aggregate interface in the root system that is bound to a nonsharable zone is dedicated to the root system, and cannot be shared. To import an interface to a vsys, the interface must be in the null zone at the root level; to export an interface from a vsys, the interface must be in the null zone at the vsys level.

At the vsys level, you can configure interfaces as described in [Table 64 on page 251](#).

**Table 64: Interface Configuration for Root and Vsys**

Interface Configuration	Description
Shared Interface	A shared interface is an interface that can be shared with the root system. To share a root interface, the interface must be shared at the root level and bound to a shared zone in a shared virtual router. By default, the untrust-vr and untrust zone are shared, enabling you to configure a vsys to share any root-level physical interface, subinterface, redundant interface, or aggregate interface that is bound to the untrust zone.
Dedicated Subinterface	A dedicated subinterface uses VLAN tagging, which enables the device to determine the vsys to which inbound or outbound traffic through that interface belongs. When you configure a subinterface in a vsys, the interface is dedicated to that vsys.
Imported Physical/Aggregate	A physical or aggregate interface in the null zone is imported from the root system, and then bound to a shared zone or the Trust-vsys_name zone. When you import a physical or aggregate interface from the root system, the vsys has exclusive use of that interface. You can also export interfaces in the null zone to the root system. When you export a interface to the root system, the root system has exclusive use of that interface.

### Using the VLAN Management Interface

To manage a vsys independent of the root system, you can create a management interface bound to the VLAN zone (automatically created when you create a vsys). Using the VLAN management interface, a vsys admin can manage the vsys using a unique IP address and VLAN ID.

You can bind more than one interface to the management zone.

- Related Documentation**
- [Virtual Router Configurations for Root and Vsys Overview on page 248](#)
  - [Viewing Root and Vsys Configurations on page 252](#)
  - [Zone Configurations for Root and Vsys Overview on page 249](#)

---

## Viewing Root and Vsys Configurations

To view a root system configuration, in the NSM navigation tree, select **Device Manager > Devices**, and then double-click the root device. To view the vsys devices associated with the root system, in the device navigation tree, select **VSYS**.

To view a vsys configuration, in the NSM navigation tree, select **Device Manager > Devices**, and then double-click the vsys. A virtual system configuration is similar to a device configuration, but a vsys configuration displays fewer settings because the root device controls some settings.

- Related Documentation**
- [Interface Configurations for Root and Vsys Overview on page 251](#)
  - [Managing Inter-Vsys Traffic with Shared DMZ Zones on page 252](#)
  - [Example: Routing Traffic to Vsys Using VLAN IDs \(NSM Procedure\) on page 252](#)

---

## Managing Inter-Vsys Traffic with Shared DMZ Zones

Virtual systems across different zones generally use a shared untrust zone for communication. However, inter-vsys traffic through a shared untrust zone is often interrupted by external traffic. To overcome such traffic interference in the shared untrust zone, you can use a shared DMZ zone created at the root level. Each shared DMZ zone that the root admin creates is automatically assigned to a shared DMZ virtual router (VR). The root admin also determines to which shared DMZ zone a particular vsys should be subscribed. A shared DMZ zone is shared only with the virtual systems that are subscribed to it. However, each vsys can be subscribed to only one shared DMZ zone. A shared DMZ zone works only on a security device running in NAT/route mode and cannot be bound to any interface other than the loopback interface. However, the default interface for the shared DMZ zone is null.

- Related Documentation**
- [Viewing Root and Vsys Configurations on page 252](#)
  - [Example: Routing Traffic to Vsys Using VLAN IDs \(NSM Procedure\) on page 252](#)
  - [Example: Routing Traffic to Vsys Using IP Classification \(NSM Procedure\) on page 255](#)

---

## Example: Routing Traffic to Vsys Using VLAN IDs (NSM Procedure)

To enable the physical device to correctly route traffic to the appropriate vsys device, you must use VLAN IDs (VIDs) at the vsys level or IP classification at the root level.

When using VIDs for routing traffic to vsys, you create dedicated vsys subinterfaces with a VID; all traffic handled by a subinterface includes the subinterface's VID in the frame



header. The root system uses the VID to correctly route traffic to and from the subinterface.



**NOTE:** A VLAN identifier is also known as a VLAN tag.

A subinterface stems from a physical interface, which acts as a trunk port. A trunk port enables a Layer 2 network device to bundle traffic from several VLANs through a single physical port, sorting the various packets by the VID in their frame headers. VLAN trunking enables one physical interface to support multiple logical subinterfaces, each of which must be identified by a unique VID. The VID on an incoming Ethernet frame indicates the destination subinterface and system. When you associate a VLAN with an interface or subinterface, the device automatically defines the physical port as a trunk port.

### Using VLANs in Transparent Mode

When the root device is in Transparent mode, you cannot use VLAN tagging at the vsys level (except when using L2V; for details, see [“Layer 2 Vsys Configuration Overview” on page 257](#)). However, you can configure subinterfaces and VLAN tagging at the root level by defining all physical ports as trunk ports. To do so, in the device navigation tree, select **Network > Interfaces**, and then double-click the VLAN-1 interface. In the General Properties interface screen, select **Vlan Trunk**.



**NOTE:** The NetScreen 5000 line of security devices running ScreenOS 5.0 L2V supports vsys transparent mode, also known as Layer 2 vsys, or L2V vsys.

In this example, you define three subinterfaces (10.1.1.1/24, 10.2.2.1/24, and 1.3.3.1/24) with VLAN tags on ethernet 2.3 for the three virtual systems vsys1, vsys2, and vsys3. The first two subinterfaces are for two private virtual systems operating in NAT mode, and the third subinterface is for a public virtual system operating in Route mode. All virtual systems share the untrust zone and its interface with the root system. The untrust zone is in the untrust-vr routing domain. For vsys1 and vsys2, you use the default virtual router. For vsys3, you choose the sharable root-level untrust-vr.

1. Add a NetScreen 5000 line of security device running ScreenOS 5.2 as the root system, and then configure the network module:
  - Double-click the device to open the device configuration. In the device navigation tree, select **Network > Slot**.
  - Double-click slot 2 to display the slot configuration dialog box. For Card Type, select **5000-8G SPM**.
  - Click **OK** to save the slot configuration.
2. Add three vsys devices:
  - Vsys1 and Vsys 2 use the default virtual router.
  - Vsys3 uses the existing untrust-vr virtual router.

- Create a subinterface for vsys1
3. In the NSM navigation tree, select **Device Manager > Devices**, and then double-click **vsys1**.
  4. In the device navigation tree, select **Network > Interfaces**. Click the **Add** icon and select **Sub Interface**.
  5. In the subinterface general properties, configure the following settings, and then click **OK**:
    - For Interface, select **ethernet2/3.1**.
    - For Sub Interface Type, select **tag**.
    - For VLAN tag, select **1**.
    - For Zone, select **trust-vsys1**.
    - For IP Address and Netmask, enter **10.1.1.1/24**.
  6. Create subinterface for vsys2:
    - In the NSM navigation tree, select **Device Manager > Devices**, and then double-click **vsys2**.
    - In the device navigation tree, select **Network > Interfaces**. Click the **Add** icon and select **Sub Interface**.
  7. In the subinterface general properties, configure the following settings, and then click **OK**:
    - For Interface, select **ethernet2/3.2**.
    - For Sub Interface Type, select **tag**.
    - For VLAN tag, select **2**.
    - For Zone, select **trust-vsys2**.
    - For IP Address and Netmask, enter **10.2.2.1/24**.
  8. Create subinterface for vsys3:
    - In the NSM navigation tree, select **Device Manager > Devices**, and then double-click **vsys3**.
    - In the device navigation tree, select **Network > Interfaces**. Click the **Add** icon and select **Sub Interface**.
    - In the subinterface general properties, configure the following settings, and then click **OK**:
      - For Interface, select **ethernet2/3.3**.
      - For Sub Interface Type, select **tag**.
      - For VLAN tag, select **3**.
      - For Zone, select **trust-vsys3**.

- For IP Address and Netmask, enter **1.3.3.1/24**.
- For Mode, select **Route**.

**Related  
Documentation**

- [Managing Inter-Vsys Traffic with Shared DMZ Zones on page 252](#)
- [Example: Routing Traffic to Vsys Using IP Classification \(NSM Procedure\) on page 255](#)
- [Layer 2 Vsys Configuration Overview on page 257](#)

## Example: Routing Traffic to Vsys Using IP Classification (NSM Procedure)

When using IP-based classification, you associate a subnet or range of IP addresses with the root or a specific vsys. The root system checks the source and destination IP addresses in IP packet headers to identify the device (root or vsys) to which traffic belongs.

You configure IP classification at the root level, on the untrust interface, which is shared by default with all vsys. In the device navigation tree of the root system, select **Network > Interfaces**, and then double-click the untrust interface. In the interface navigation tree, select **IP Classification**, and then select **Enabled**. Right-click and select **New** to display the New IP Classification List, and then configure a subnet or IP address range for the root and/or each vsys.

In this example, you configure IP-based traffic classification for three virtual systems (vsys1, vsys3, and vsys3). You define the trust-vr as sharable, and then create a shared zone called internal that is bound to the trust-vr (both internal and untrust zones are in the shared trust-vr routing domain). Within the internal zone, configure a subnet for each vsys (10.1.1.0/24 for vsys1, 10.1.2.0/24 for vsys2, and 10.1.3.0/24 for vsys3).

Next, bind the interfaces. Configure ethernet1/1 in the shared internal zone, assign IP address 10.1.0.1/16, and select NAT mode. Configure ethernet1/2 in the shared untrust zone and assign it IP address 210.1.1.1/24. Finally, configure the default gateway in the untrust zone as 210.1.1.250.

1. Add an ISG2000 security device running ScreenOS 5.2 as the root system, and then configure the network module:
  - Double-click the device to open the device configuration. In the device navigation tree, select **Network > Slot**.
  - Double-click slot 1 to display the slot configuration dialog box. For Card Type, select **8 Interfaces (10/100)**.
2. Click **OK** to save the slot configuration.
3. Add the following vsys devices (all use default virtual router):
  - vsys1
  - vsys2

- **vsys3**
  - In the device navigation tree, select **Network > Virtual Routers**, and then double-click **trust-vr**. Ensure that Shared Virtual Router is selected, and then click **OK**.
4. In the device navigation tree, select **Network > Zones**. Click the **Add** icon and select **New Security Zone**. In the Zone General Properties, configure the following settings:
    - For Name, enter **internal**.
    - For Virtual Router, select **trust-vr**.
    - Select **Shared**. When selected, the option IP Classification appears in the zone navigation tree.
    - In the zone navigation tree, select **IP Classification**, and then configure the following settings:
      - Select **Enabled**.
  5. Right-click in the IP Classification screen and select **New**. The New IP Classification list appears. Configure the following settings, and then click **OK**:
    - For Vsys, select **vsys1**.
    - Select **Subnet**.
    - For IP Address and Netmask, enter **10.1.1.0/24**.Right-click in the IP Classification screen and select **New**. The New IP Classification list appears. Configure the following settings, and then click **OK**:
    - For Vsys, select **vsys2**.
    - Select **Subnet**.
    - For IP Address and Netmask, enter **10.1.2.0/24**.
  6. Right-click in the IP Classification screen and select **New**. The New IP Classification list appears. Configure the following settings, and then click **OK**:
    - For Vsys, select **vsys3**.
    - Select **Subnet**.
    - For IP Address and Netmask, enter **10.1.3.0/24**.
    - In the device navigation tree, select **Network > Interfaces**
  7. Double-click **ethernet 1/1**. In the Interface General Properties, configure the following settings, and then click **OK**:
    - For Zone, select **internal**.
    - For IP Address and Netmask, enter **10.1.0.1/16**.
  8. Double-click **ethernet 1/2**. In the Interface General Properties, configure the following settings, and then click **OK**:

- For Zone, select **Untrust**.
  - For IP Address and Netmask, enter **210.1.1.1/24**.
  - In the device navigation tree, select **Network > Virtual Routers**, and then double-click **trust-vr**.
  - In the virtual router navigation tree, select **Routing Table**.
9. In the Destination-based Routing Table area, click the **Add** icon. Configure the following route, and then click **OK**:
- For IP Address and Netmask, enter **0.0.0.0/0**.
  - For Next Hop, select **Gateway**.
  - For Interface, select **ethernet1/2**.
  - For Gateway IP Address, enter **210.1.1.250**.

**Related  
Documentation**

- [Layer 2 Vsys Configuration Overview on page 257](#)
- [Example: Routing Traffic to Vsys Using VLAN IDs \(NSM Procedure\) on page 252](#)
- [Assigning L2V VLAN IDs \(NSM Procedure\) on page 258](#)

## Layer 2 Vsys Configuration Overview

A NetScreen 5000 line of security device running ScreenOS 5.0-L2V supports virtual systems in Transparent mode (the device functions similar to a Layer 2 switch or bridge). The device groups packets to or from a unique vsys based on the VLAN tag in the packet header, applies the security policy for the vsys to the packets, and then sends permitted packets through the device without packet modification.

When you first add a NetScreen 5000 line of security device running ScreenOS 5.0-L2V to NSM, the device is in neutral mode, meaning that neither L2V or VLAN trunk mode is configured on the device. To confirm that the device is neutral mode, ensure that the root system does not contain a VLAN group, no VLAN IDs have been exported to a vsys device, `vlan1` exists in the root system only, and that the VLAN trunk mode is disabled.

To enable L2V on a neutral root system, you must:

1. Import VLAN IDs from the root system to vsys.
2. Create a VLAN group (in the root system or vsys) and assign that group to a physical port and zone.

When L2V is enabled, you cannot configure VLAN trunk mode (option is disabled). For information about how to change an L2V root system to VLAN trunk mode, see [“Converting L2V to VLAN Trunking \(NSM Procedure\)” on page 261](#).

**Related  
Documentation**

- [Assigning L2V VLAN IDs \(NSM Procedure\) on page 258](#)
- [L2V VLAN Groups in NSM Overview on page 258](#)

- [Example: Routing Traffic to Vsys Using IP Classification \(NSM Procedure\) on page 255](#)

---

## Assigning L2V VLAN IDs (NSM Procedure)

---

You must use VLAN tags for vsys devices in Transparent mode. The device classifies traffic to or from the vsys based on the VLAN tag. A root device running ScreenOS 5.0-L2V supports a maximum of 4094 VLANs. You can assign each vsys 2 to 4094 VLANs, however, after a VLAN is assigned to one vsys it cannot be used in another. The root system reserves vlan 1, vlan0, and vlan4095.

By default, all VLAN IDS belong to the root system. To configure VLAN IDs for each vsys, you must import the VLAN IDs from the root system to a vsys:

1. In the NSM navigation tree, select **Device Manager > Security Devices**, and then double-click a vsys device.
2. In the vsys device navigation tree, select **Network > Vlan > Import**.
3. Click the **Add** icon to display the New Vlan Import Entry dialog box, and then enter the range of VLAN IDs you want to import from the root system to the vsys.
4. Click **OK**. NSM imports the VLAN IDs within the specified range from the root system; these IDs are now reserved and cannot be used by the root system or other vsys.

To export VLAN IDs to the root system, you must delete the VLAN IDs from the vsys (select the VLAN import entry and then click the **Delete** icon). When you delete an ID range, NSM no longer reserves those IDs, enabling you to import the IDs to another vsys.

After you have imported VLAN IDs to a vsys, you can group those IDs and assign them to a physical port and zone.

### Related Documentation

- [L2V VLAN Groups in NSM Overview on page 258](#)
- [Predefined L2V Zones in NSM Overview on page 259](#)
- [Layer 2 Vsys Configuration Overview on page 257](#)

---

## L2V VLAN Groups in NSM Overview

---

A VLAN group contains VLAN IDs and specifies the port and zone on the physical device that handles those IDs. You can create a VLAN group that includes a single ID range, or add multiple ID ranges to group multiple VLAN ranges.

For each group, you must configure:

- The VLAN IDs ranges you want to include in the group. To include an ID range within a group, you must have previously imported the IDs to the vsys (the IDs must be reserved by the vsys). To view the VLAN IDs imported to the vsys, select the option **Show Vlan IDs Imported** (option is located at the bottom of the VLAN Group screen). To clear the VLAN ID information from the group screen, clear (unselect) the option.

- The port and zone that handle traffic with the specified IDs. You can select any physical interface or aggregate interface and any L2 zone. Interfaces included within an aggregate interface are not displayed and cannot be selected.

If you select the null zone for a VLAN interface, NSM automatically sets the zone as v1-null.

You can create VLAN groups at the root level and at the vsys level. When configuring a root VLAN group, however, any VLAN ID ranges you include in the group are automatically reserved for the root system and cannot be imported by a vsys.

You cannot delete VLAN IDs that are included in a VLAN group.

#### Related Documentation

- [Predefined L2V Zones in NSM Overview on page 259](#)
- [L2V Interface Management in NSM Overview on page 260](#)
- [Assigning L2V VLAN IDs \(NSM Procedure\) on page 258](#)

## Predefined L2V Zones in NSM Overview

You can configure any predefined zone in a shared virtual router as shareable. In the NSM UI, the following predefined L2 zones appear with regular zone names:

- v1-trust appears as trust
- v1-untrust appears as untrust
- v1-dmz appears as dmz

The exception is v1-null, which appears as v1-null; the regular null zone is unchanged, and appears as null. By default, the predefined VLAN zone is also sharable when using L2V. The VLAN zone contains all vsys management interfaces.

You can also create custom L2V zones in the root system or vsys, although you cannot configure a custom L2V zone as sharable. When you define a new L2 zone, NSM prepends the prefix “L2-” to the name during a device update. However, the L2 prefix does not appear in the NSM UI. For example, if you create an L2 zone named “music,” the UI displays the zone name as “music,” but the Web UI and CLI displays the zone name as “L2-music.”



**NOTE:** When configuring a custom L2V zone, the name must include only lowercase letters.

#### Related Documentation

- [L2V Interface Management in NSM Overview on page 260](#)
- [Converting L2V to VLAN Trunking \(NSM Procedure\) on page 261](#)
- [L2V VLAN Groups in NSM Overview on page 258](#)

## L2V Interface Management in NSM Overview

In the root system, you can bind any interface to an L2 zone. If the zone is shared with vsys, the interface also becomes shared with vsys. You cannot import or export interfaces between root and vsys, and you cannot assign an IP address to an interface (except the VLAN management interfaces).

In the root system, you can create VLAN management interfaces and aggregate interfaces. At the vsys level, you can only create VLAN management interfaces. The topic includes the following:

- [Configuring L2V VLAN Management Interfaces on page 260](#)
- [Configuring L2V Aggregate Interfaces on page 260](#)

### Configuring L2V VLAN Management Interfaces

The root system contains a predefined VLAN management interface (vlan1) that is bound to the VLAN zone. You can configure this interface as you would a normal security interface, for example, assign the interface an IP address, configure DHCP, or configure monitoring.

For each vsys that you want to manage, you must create the VLAN management interface on the vsys, and then bind the interface to the VLAN zone. Because each VLAN interface uses a VLAN ID, you must have previously imported VLAN IDs from a root system before creating the VLAN interface on a vsys device. For example, before you create vlan.3 management interface on a vsys, you must import the VLAN ID 3 from the root system.

For both root and vsys, the VLAN interface name is the VLAN ID for the interface. To add multiple management interfaces, bind each interface to the VLAN zone and assign each interface a unique vlan name (vlan1, vlan2, vlan3, and so on; acceptable range is 2-4094 only in Transparent mode). When assigning IP address to each interface, ensure that the IP subnets for all interfaces do not overlap.

### Configuring L2V Aggregate Interfaces

You can create aggregate interfaces in the root system to increase available bandwidth. An aggregate interface must be bound to an L2 zone (cannot be bound to the VLAN zone) and can be shared with vsys. Although you can manage this interface, you cannot assign an IP address. Additionally, if you bind a regular interface to an L2 aggregate interface, you cannot select the zone for the regular interface. You cannot create aggregate interfaces at the vsys level.

The 8G Secure Port Module (SPM) supports two ASICs; ports ethernet2/1 through ethernet2/4 use one ASIC, and ports ethernet2/5 through ethernet2/8 use the other. You must configure aggregate interfaces in pairs, starting with port ethernet2/1.

**Table 65: L2V Aggregate Interfaces**

Aggregate Interface	Ports
aggregate1	ethernet2/1 and ethernet2/2



Table 65: L2V Aggregate Interfaces (*continued*)

Aggregate Interface	Ports
aggregate1	ethernet2/3 and ethernet2/4
aggregate1	ethernet2/5 and ethernet2/6
aggregate1	ethernet2/7 and ethernet2/8

The 8G2 Secure Port Module (SPM) supports a maximum of two 4-port aggregate interfaces, four trusted and four untrusted. Assigning the VLANs to an aggregate interface provides a traffic bandwidth of 2 Gbps in each direction, with a maximum of 4 Gbps for bidirectional traffic per Application-Specific Integrated Circuit (ASIC). You must configure aggregate interfaces in pairs, starting with port ethernet2/1, as shown in

[Table 66 on page 261](#).

Table 66: 8G2 SPM and the 5000M2 Management Module

Aggregate	Ports
aggregate1	ethernet2/1, ethernet2/2, ethernet2/3, and ethernet2/4
aggregate2	ethernet2/5, ethernet2/6, ethernet2/7, and ethernet2/8

- Related Documentation**
- [Converting L2V to VLAN Trunking \(NSM Procedure\) on page 261](#)
  - [L2V VLAN Groups in NSM Overview on page 258](#)
  - [Predefined L2V Zones in NSM Overview on page 259](#)

## Converting L2V to VLAN Trunking (NSM Procedure)

When the VLAN interface is set to Trunk mode, the root system operates in VLAN trunk mode and L2V is disabled for the device. While in VLAN Trunk mode, all L2V functionality is unsupported: You cannot import VLAN IDs to vsys devices or VLAN groups to root or vsys.

To change a neutral root system to VLAN Trunk mode, in the device navigation tree, select **Network > Interfaces**, and then double-click the vlan1 interface. In the General Properties interface screen, select **Vlan Trunk**. To disable VLAN Trunk mode, clear the Vlan Trunk option (the device returns to neutral).

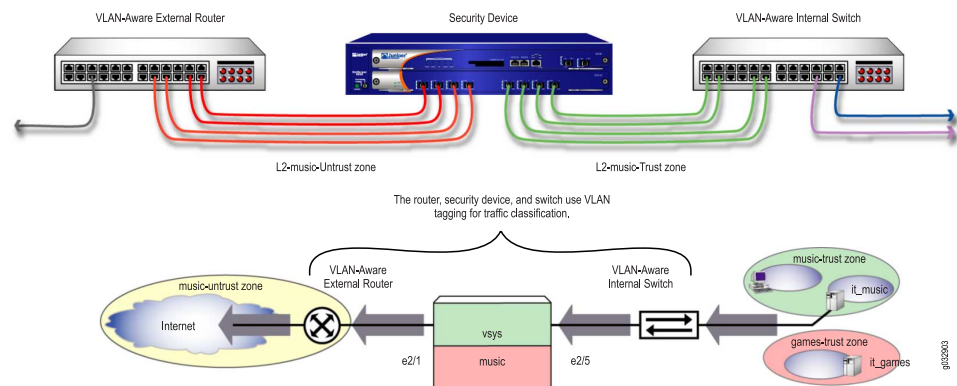
To change an L2V root device to VLAN Trunk mode, you must first delete VLAN IDs that were imported to vsys devices and VLAN groups in the root and vsys devices.



**NOTE:** To confirm that the device is in neutral mode, ensure that the root system does not contain a VLAN group, no VLAN IDs have been exported to a vsys device, vlan1 exists in the root system only, and that the VLAN trunk mode is disabled.

In this example, you configure a NetScreen-5200 security device in L2V mode and the vsys “music.” The music vsys shares the music-untrust zone with the root system. You must import the VLANs to a vsys before they can be tagged. [Figure 4 on page 262](#) describes the single port L2V configuration.

**Figure 4: Example Single Port L2V Configuration**



1. Add a NetScreen 5000 line of security device in Transparent mode running ScreenOS 5.0 L2V as the root system, and then configure the network module:
  - Double-click the device to open the device configuration. In the device navigation tree, select **Network > Slot**.
  - Double-click slot 2 to display the slot configuration dialog box. For Card Type, select **5000-8G SPM**.
  - Click **OK** to save the slot configuration.
  - Create the vsys music. In the Device Manager, select **Security Devices**, and then double-click the vsys music to open the vsys configuration.
2. Create two custom Layer 2 zones on the vsys music:
  - In the vsys configuration tree, select **Network > Zones**. Click the **Add** icon and select **Security Zone**. Configure the zone name as music-trust, and then click **OK**.
  - In the vsys configuration tree, select **Network > Zones**. Click the **Add** icon and select **Security Zone**. Configure the zone name as music-untrust, and then click **OK**.
3. Import VLAN IDs from the root system to the vsys music:
  - In the vsys navigation tree, select **Network > Vlan > Import**.
  - Click the **Add** icon to display the New VLAN Import Entry. Configure the following settings, and then click **OK**:

- For Vlan ID Begin, enter **100**.
  - For Vlan ID End, enter **199**.
  - For Comments, enter **music vlans**.
  - Create a VLAN group on the vsys music. In the vsys navigation tree, select **Network > Vlan > Group**, and then click the **Add** icon to display the New VLAN Group Entry. Configure the following setting:
    - For Vlan Group Name, enter **it\_music**.
4. In the Setting Vlan Group area, click the **Add** icon to display the New Vlan Group Range. Configure the following settings, and then click **OK**:
    - For Start Vlan ID, enter **100**.
    - For End Vlan ID, enter **199**.
  5. In the Binding Vlan Group to Port and Zone area, click the **Add** icon to display the New Vlan Group Port Settings. Configure the following settings, and then click **OK**.
    - For Interface, select **ethernet2/5**.
    - For Zone, select **music-trust**.
  6. In the Binding Vlan Group to Port and Zone area, click the **Add** icon to display the New Vlan Group Port Settings. Configure the following settings, and then click **OK**.
    - For Interface, select **ethernet2/1**.
    - For Zone, select **music-untrust**.
    - Create management interface for vsys music:
      - In the vsys navigation tree, select **Network > Interfaces**, and then click the **Add** icon and select **VLAN Interface**.
  7. Configure the following General Properties:
    - For Name, enter **199** (name appears as vlan199).
    - For Zone, select **vlan**.
    - For IP Address/Netmask, enter **1.0.1.199/24**.
    - Clear the **Manageable** check box.
    - In the interface navigation tree, select **Service Options**. Select **Telnet**, **Ping**, and **Web**, and then click **OK**:
  8. Configure zone firewall rules in a security policy for vsys music. First, create a rule that permits HTTP traffic from music-untrust to music trust:
    - For From zone, select **music-untrust**.
    - For Source Address, select **any**.
    - For To zone, select **music-trust**.
    - For Destination Address, select **any**.

- For Service, select **HTTP**.
  - For Action, select **Permit**.
  - For Install On, right-click and select **Select Target**. In the Select Target Devices list, select **vsys music**, and then click **OK**.
9. Create a rule that denies all traffic from music-untrust to music trust:
- For From zone, select **music-untrust**.
  - For Source Address, select **any**.
  - For To zone, select **music-trust**.
  - For Destination Address, select **any**.
  - For Service, select **any**.
  - For Action, select **deny**.
  - For Install On, right-click and select **Select Target**. In the Select Target Devices list, select **vsys music**, and then click **OK**.
10. Create a rule that permits all traffic from music-trust to music untrust:
- For From zone, select **music-trust**.
  - For Source Address, select **any**.
  - For To zone, select **music-untrust**.
  - For Destination Address, select **any**.
  - For Service, select **any**.
  - For Action, select **Permit**.
  - For Install On, right-click and select **Select Target**. In the Select Target Devices list, select **vsys music**, and then click **OK**.
11. From the menu bar, select **File > Assign Policy**. In the Assign Policy to Devices list, select **vsys music**, and then click **OK**.

**Related  
Documentation**

- [Predefined L2V Zones in NSM Overview on page 259](#)
- [L2V Interface Management in NSM Overview on page 260](#)

---

## Configuring Crypto-Policy Overview

In public key cryptography, a public/private key pair is used to encrypt and decrypt data. Data encrypted with a public key, which the owner makes available to the public, can only be decrypted with the corresponding private key, which the owner keeps secret and protected. For example, if Alice wants to send Bob an encrypted message, Alice can encrypt it with Bob's public key and send it to him. Bob then decrypts the message with his private key.

The reverse is also useful; that is, encrypting data with a private key and decrypting it with the corresponding public key. This is known as creating a digital signature. For example, if Alice wants to present her identity as the sender of a message, she can encrypt the message with her private key and send the message to Bob. Bob then decrypts the message with Alice's public key, thus verifying that Alice is indeed the sender.

Public/private key pairs also play an important role in the use of digital certificates.

If Negotiation mode for the IKEV1, Encryption ALG, Authentication ALG, DH Group, and Authentication Method options are disabled, then these parameters do not provide any restriction.



**NOTE:** Although these configurations cannot be set in vsys devices, a vsys device can use these configurations through root devices that share them.

There are three types of administrators who can configure crypto-policy. They are:

- A root administrator
- A read-write admin user without any role attribute assigned
- A read-write admin user with a cryptographic role

#### Related Documentation

- [Certificate Authentication Support in NSM Overview on page 265](#)
- [Self-Signed Certificates in NSM Overview on page 266](#)
- [Converting L2V to VLAN Trunking \(NSM Procedure\) on page 261](#)

## Certificate Authentication Support in NSM Overview

Every security device supports the use of certificates to authenticate itself to outside parties. A digital certificate is an electronic means for verifying identity through a trusted third party, known as a certificate authority (CA). The CA is a trusted partner of the identity sending the digital certificate as well as the identity receiving it. To authenticate identity, the CA issues certificates, often with a set time limit. If you do not renew the certificate before the time limit is reached, the CA considers the certificate inactive. For example, a VPN member attempting to use an expired certificate is immediately detected (and rejected) by the CA.

You can use certificates to authenticate a VPN member (external device or security device), RAS users for a group IKE ID, or SSL management of a security device. You must obtain and install the following certificates on the managed device before you can use certificates to authenticate the device:

- [“Local Certificate Validation of ScreenOS Devices Overview” on page 266](#)—A local certificate authenticates the identity of the device on which it is installed.
- [“Certificate Authority Configuration in NSM Overview” on page 271](#)—A CA certificate authenticates a third party.

- [“Configuring Certificate Revocation Lists \(NSM Procedure\)” on page 273](#) (Optional)—A certificate revocation list (CRL) ensures that expired certificates are not accepted.



**NOTE:** A CRL is optional; you do not need to obtain and install a CRL on the security device to use certificates.

When you import a security device that already has a local certificate, CA, and CRL installed, these certificates and lists are automatically imported as part of the device configuration when you add that device to the NSM system. However, to reuse the CA and CRL in other security devices, you must load the CA and CRL file directly into the management system (you cannot reuse a local certificate on another device). For information, see [“Imported Certificates in NSM Overview” on page 273](#).

**Related Documentation**

- [Self-Signed Certificates in NSM Overview on page 266](#)
- [Local Certificate Validation of ScreenOS Devices Overview on page 266](#)
- [Configuring Crypto-Policy Overview on page 264](#)

---

## Self-Signed Certificates in NSM Overview

For devices running ScreenOS 5.1 and later, a self-signed certificate is automatically created each time the device powers on; you can use this self-signed certificate to authenticate the device for SSL management. Because this self-signed certificate is not authenticated by an external, third-party certificate authority, you cannot use it to authenticate a VPN member in an IKE VPN. A device running ScreenOS 5.1 and later automatically creates the self-signed certificate upon reboot, so you do not need to configure a Generate Certificate Request to obtain it. However, if you delete the self-signed certificate for a device and do not want to reboot the device to obtain a new certificate, you can use the Generate Certificate Request procedure to prompt the device to regenerate the certificate. For steps to obtain a self-signed certificate, see [“Generating Certificate Requests to ScreenOS Devices \(NSM Procedure\)” on page 267](#).

A self-signed certificate that was automatically generated by the device at startup has a certificate status of *system*. If you use the Generate Certificate Request to obtain a new self-signed certificate, the self-signed certificate has a certificate status of *active*.

**Related Documentation**

- [Local Certificate Validation of ScreenOS Devices Overview on page 266](#)
- [Generating Certificate Requests to ScreenOS Devices \(NSM Procedure\) on page 267](#)
- [Certificate Authentication Support in NSM Overview on page 265](#)

---

## Local Certificate Validation of ScreenOS Devices Overview

A local certificate validates the identity of the security device. Each security device that performs authentication (in a VPN, for SSL management, for device administrators) must have a local certificate installed on the device. To view the available local certificates on a device, in the device navigation tree, select **VPN Settings > Local Certificates**.

To get a local certificate for a device, you must prompt the device to generate a certificate request (includes public/private key pair request) using the Generate Certificate Request directive. Depending on how you want to use the local certificate and the version of ScreenOS the device is running, you can configure a CA-signed local certificate or a self-signed local certificate as described in [Table 67 on page 267](#).

**Table 67: Local Certificate Validation**

Local Certificate Types	Description
Obtain a local certificate signed by a CA	Use for devices running ScreenOS 5.0 or later, and for devices running ScreenOS 5.1 and later that need to use a local certificate for authentication in an IKE VPN. When the device receives the prompt for a certificate request, it processes the request and returns the encrypted public key for the device. Using this encrypted public key, you can contact an independent CA (or use your own internal CA, if available) to obtain a local device certificate file (a .cer file). You must install this local certificate file on the managed device using NSM before you can use certificates to validate that device. Because the local certificate is device-specific, you must use a unique local certificate for each device.
Use the self-signed certificate	Use for devices running ScreenOS 5.1 and later that do not need to use the certificate for authentication in an IKE VPN. When configuring the request, select <b>Create Self-Signed Certificate</b> . When the device receives the certificate request, it processes the request and automatically adds the certificate to the device. Because this certificate is both a local and CA certificate, you do not need to contact a CA.

For CA-signed local certificates, you can also use SCEP to configure the device to automatically obtain a local certificate (and a CA certificate) from the CA directly.

**Related Documentation**

- [Generating Certificate Requests to ScreenOS Devices \(NSM Procedure\) on page 267](#)
- [Loading Local Certificate into NSM Management System on page 269](#)
- [Self-Signed Certificates in NSM Overview on page 266](#)

## Generating Certificate Requests to ScreenOS Devices (NSM Procedure)

To send a certificate request prompt to the managed device, right-click the device and select **Certificates > Generate Certificate Request**. Enter the information as described in [Table 68 on page 267](#).

**Table 68: Certificate Requests**

Certificate Requests	Your Action
Name	Enter the name of the certificate requestor; typically, this is the person who administrators the security device.
Phone	Enter the telephone number of the certificate requestor.
Domain Component	Enter one or more domain components for the certificate requestor. Multiple entries must be separated by commas.
Unit/Department	Enter the unit or department of the certificate requestor.

Table 68: Certificate Requests (*continued*)

Certificate Requests	Your Action
Organization	Enter the organization of the certificate requestor.
County/Locality	Enter the county or locality of the certificate requestor.
State	Enter the state of the certificate requestor.
Country	Enter the country of the certificate requestor.
E-mail	Enter the e-mail address of the certificate requestor.
IP Address	Enter the IP address of the certificate requestor.
FQDN	Enter the fully qualified domain name of the security device.
Key Pair Type	Select RSA or DSA encryption.
Key Pair Length	Select the key length: 512, 768, 1024, or 2048. Ensure that your certificate authority can support the key length you select. Key lengths greater than 1024 might require generation times longer than 10 minutes.
Create Self-Signed Certificate (ScreenOS 5.1 and higher only)	Select this option to use the self-signed certificate on a device running ScreenOS 5.1 and later. Because the self-signed certificate is both the local certificate and the CA certificate, when this option is enabled the SCEP options are automatically disabled.
Automatically Enroll	<p>Select this option to use SCEP. The device automatically requests, receives, and installs the local certificate and the CA certificate locally. To use SCEP, configure the following defaults:</p> <ul style="list-style-type: none"> <li>• Certificate authority—Select a preconfigured CA or use the default CA settings for the device.</li> <li>• E-mail request to—Provide the e-mail address that receives the PKCS#10 file, which defines the syntax for certification requests.</li> </ul>

Click **OK** to send the request prompt to the device.

A Job Manager window appears to display job information and job progress. When the job is complete, the device public key appears in the Job window.

If you are obtaining the local certificate manually, you need the device public key to give to the CA. Copy and paste the information from the job window to a text file, or leave the job window open while you contact the CA.

If you are using SCEP to obtain a local certificate and a CA certificate, the device automatically sends its public key to the CA directly. When SCEP obtains both the local and CA certificate, the job completes. Close the Job Manager window, and then check the status of certificates: open the device configuration and select **VPN Settings > Local Certificates**. The certificate status appears as *active*, indicating that the certificate file has been successfully installed on both the physical device and the management system (you might need to use the Refresh directive to prompt the UI to update the certificate status).



If you are using the self-signed certificate on a device running ScreenOS 5.1 and later, the device automatically creates the certificate. A Job Manager window appears to display job information and job progress. When the job is complete, close the Job Manager window. To view the certificate, open the device configuration and select **VPN Settings > Local Certificates**. The certificate status appears as *active*, indicating that the self-signed certificate file has been successfully created and installed on both the physical device and the management system.

**Related Documentation**

- [Loading Local Certificate into NSM Management System on page 269](#)
- [Installing Local Certificates Using SCEP in NSM on page 270](#)
- [Local Certificate Validation of ScreenOS Devices Overview on page 266](#)

## Loading Local Certificate into NSM Management System

For CA-signed local certificates, after you prompt the device to generate the certificate request, the device creates the public/private key pair that is used to create the local certificate and returns the public key to the management system (the private key never leaves the device). During this time, the certificate status is *key pair*, meaning that a key pair exists but no certificate has been loaded.

After you obtain the local certificate, you must load the certificate into the management system using the NSM UI, and then install the certificate on the managed device:

- For devices running ScreenOS 5.x, you must install a TFTP server on the NSM device server. The device server automatically uses TFTP to load the certificate onto your managed devices. For more information about creating a TFTP server on the device server, see the *Network and Security Manager Installation Guide*.
- For devices running ScreenOS 5.1 and later, 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 NSM device server.

After the certificate is installed on the device, the certificate is known as *active*. To view the current status of your certificate requests, open the device configuration and select **VPN Settings > Local Certificates**:

- Before the certificate is fulfilled, the certificate status appears as *key pair*, indicating a public/private key pair exists but the certificate file does not yet exist on both the physical device and the management system.
- After the certificate is fulfilled, the certificate status appears as *active*, indicating that the certificate file has been successfully installed on both the physical device and the management system.



**NOTE:** Any time you need to move information from the physical device to the management system, you are using a Refresh directive; when you need to move information from the management system to the physical device, you are using an Update directive.

- Related Documentation**
- [Installing Local Certificates Using SCEP in NSM on page 270](#)
  - [Manual Installation of Local Certificates in NSM on page 270](#)
  - [Generating Certificate Requests to ScreenOS Devices \(NSM Procedure\) on page 267](#)

---

## Installing Local Certificates Using SCEP in NSM

If you used SCEP for automatic enrollment, the device contacts the specified CA and obtains a local and CA certificate. After the device has installed the certificate, refresh the NSM device configuration for that device to view the new certificate information:

1. Right-click the device and select **Certificates > Refresh Local Certificates**. This directive uses the information about the physical device to refresh the information on the management system.
2. Double-click the device configuration and then select **VPN Settings > Local Certificates** to view the local certificates. The certificate status appears as *active*, indicating that the certificate file has been successfully installed on both the physical device and the management system.

- Related Documentation**
- [Manual Installation of Local Certificates in NSM on page 270](#)
  - [Certificate Authority Configuration in NSM Overview on page 271](#)
  - [Loading Local Certificate into NSM Management System on page 269](#)

---

## Manual Installation of Local Certificates in NSM

If you did not use SCEP, you must manually contact your CA and use the device public key to create a local device certificate. After you have obtained the local certificate (.cer) file from your CA, install that certificate on the device:

1. Right-click the device and select **Certificates > Update Fulfilled Certificate**. This directive uses the information in the management system to update the information about the physical system.
2. Load the certificate file and click **OK** to install the local certificate on the device.



.....

**NOTE:** For devices running ScreenOS 5.x, you must install a TFTP server on the NSM device server. The device server automatically uses TFTP to load the local certificate onto your managed devices. For more information about creating a TFTP server on the device server, see the *Network and Security Manager Installation Guide*.

.....

A Job Manager window appears to display job information and job progress. When the job is complete, close the Job Manager window.

3. View the local certificate by double-clicking the device configuration and selecting **VPN Settings > Local Certificates**. The certificate status appears as *active*, indicating

that the certificate file has been successfully installed on both the physical device and the management system.

For devices running ScreenOS 5.1 and later, the device server automatically uses Secure Server Protocol (SSP) (the protocol used for the management connection) to load the local certificate.

**Related  
Documentation**

- [Certificate Authority Configuration in NSM Overview on page 271](#)
- [Installing CA Certificates Using SCEP in NSM on page 271](#)
- [Installing Local Certificates Using SCEP in NSM on page 270](#)

## Certificate Authority Configuration in NSM Overview

A CA certificate validates the identity of the third party CA that issued the local device certificate. To view the available CA certificates on a device, in the device navigation tree, select **VPN Settings > CA Certificates**.



**NOTE:** If you are using a self-signed certificate, you do not need to contact a CA. The self-signed certificate on the device is issued and signed by the same entity (the device), so the issuer and the subject of the certificate are the same. However, because this self-signed certificate is not authenticated by an external, third-party certificate authority, you cannot use it to authenticate a VPN member in an IKE VPN.

To obtain a CA certificate file (.cer), contact the CA that issued the local certificate, then use this file to create a certificate authority object. You must install this CA certificate on the managed device using NSM 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” in the *Network and Security Manager Administration Guide*.

**Related  
Documentation**

- [Installing CA Certificates Using SCEP in NSM on page 271](#)
- [Manual Installation of CA Certificates in NSM on page 272](#)
- [Manual Installation of Local Certificates in NSM on page 270](#)

## Installing CA Certificates Using SCEP in NSM

If you used SCEP to obtain a local certificate for the device, the CA certificate was automatically downloaded and installed on the device at the same time as the local

certificate. However, because the management system does not know about the CA certificate, you must refresh the CA information:

1. Right-click the device and select **Certificates > Refresh CA Certificates**. This directive uses the information about the physical device to refresh the information on the management system.
2. Open the device configuration to view the CA certificates in **VPN Settings > CA Certificates**.

**Related  
Documentation**

- [Manual Installation of CA Certificates in NSM on page 272](#)
- [Configuring Certificate Revocation Lists \(NSM Procedure\) on page 273](#)
- [Certificate Authority Configuration in NSM Overview on page 271](#)

---

## Manual Installation of CA Certificates in NSM

If you did not use SCEP, you must manually contact your CA, obtain a CA certificate, and create a certificate authority Object. Then, add the CA certificate to the device and install it on the device:

1. Open the device configuration and select **VPN Settings > CA Certificates**. Click the **Add** icon and add the certificate authority object. Close the device configuration.
2. Right-click the device and select **Certificates > Update CA Certificate**. This directive uses the information in the management system to update the information on the physical system. A Job Manager window appears to display job information and job progress.



.....

**NOTE:** For devices running ScreenOS 5.x, you must install a TFTP server on the NSM device server. The device server automatically uses TFTP to load the CA certificate onto your managed devices. For more information about creating a TFTP server on the device server, see the *Network and Security Manager Installation Guide*.

.....

3. When the job is complete, close the Job Manager window.

For devices running ScreenOS 5.1 and later, the device server automatically uses Secure Server Protocol (SSP) (the protocol used for the management connection) to load the CA certificate.

To view CA certificate, open the device configuration and select **VPN Settings > CA Certificates**.

**Related  
Documentation**

- [Configuring Certificate Revocation Lists \(NSM Procedure\) on page 273](#)
- [Imported Certificates in NSM Overview on page 273](#)
- [Installing CA Certificates Using SCEP in NSM on page 271](#)

## Configuring Certificate Revocation Lists (NSM Procedure)

A certificate revocation list (CRL) identifies invalid certificates. To view the available CRLs on a device, in the device navigation tree, select **VPN Settings > CRLs**. To obtain a CRL file (.crl), contact the CA that issued the local certification and CA certificate for the device, then use this file to create a Certificate Revocation List object.

You must install the CRL on the managed device using NSM before you can use a CRL to check for revoked certificates in your VPN. Because the CRL is an object, however, you can use the same CRL for multiple devices, as long as those devices use local and CA certificates that were issued by that CA. After you have received a CRL, you can use the CRL object in your VPN. For details on configuring a certificate revocation list object, see [“Configuring CRL Objects” on page 216](#).

You must manually contact your CA, obtain a CRL, and create a certificate revocation list object. Then, add the CRL to the device and install it on the device:

1. Open the device configuration and select **VPN Settings > CRLs**. Click the **Add** icon and add the Certificate Revocation List object. Close the device configuration.
2. Right-click the device and select **Certificates > Update CRL**. This directive uses the information in the management system to update the information on the physical system. A Job Manager window appears to display job information and job progress.



**NOTE:** For devices running ScreenOS 5.x, you must install a TFTP server on the NSM device server. The device sServer automatically uses TFTP to load the CRL onto your managed devices. For more information about creating a TFTP server on the device server, see the *Network and Security Manager Installation Guide*.

3. When the job is complete, close the Job Manager window.

For devices running ScreenOS 5.1 and later, the device server automatically uses Secure Server Protocol (SSP) (the protocol used for the management connection) to load CRLs.

To view CRL, double-click the device configuration and select **VPN Settings > CRL**.

### Related Documentation

- [Imported Certificates in NSM Overview on page 273](#)
- [Manual Installation of CA Certificates in NSM on page 272](#)
- [PKI Default Settings Configuration in NSM Overview on page 274](#)

## Imported Certificates in NSM Overview

If you imported a security device that already has a local certificate, CA, and CRL, these objects are automatically imported when you add that device to the NSM system. Imported objects use the default name of `<CN>_<timestamp>`.

However, to reuse the CA and CRL objects in other security devices, you must load the CA and CRL file directly into the management system:

- To load a CA file (.cer) into the management system, open the imported CA object in Object Manager and use the Load Certificate option. After loading the CA, verify the status of the certificate appears as Loaded.
- To load a CRL file (.crl) into the management system, open the imported CRL object in Object Manager and use the Load CRL option. After loading the CRL, verify the status of the CRL appears as Loaded.

After the CA certificate and CRL files have been loaded, you can use those CA and CRL objects in other devices.

**Related  
Documentation**

- [PKI Default Settings Configuration in NSM Overview on page 274](#)
- [Configuring Certificate Revocation Lists \(NSM Procedure\) on page 273](#)

---

## PKI Default Settings Configuration in NSM Overview

You can configure default PKI settings for each security device to define how that device handles certificates. When configuring a VPN that includes the device, you can use these default settings.

In the device configuration tree, select **VPN Settings > Defaults > PKI Settings** to display the default PKI settings. First, configure the source interface for PKI traffic. The source interface is the interface on the device that sends the certificate request to the CA. The topic includes the following:

- [Configuring X509 Certificates on page 274](#)
- [Configuring Revocation on page 274](#)
- [Configuring Simple Certificate Enrollment Protocol on page 275](#)

### Configuring X509 Certificates

Configure the following X509 certificate settings:

- Email Destination for the PKCS#10 File—Provide the e-mail address that receives the PKCS#10, which defines the syntax for certification requests.
- Select raw common name—Select this option to use only one CN field in the certificate CN in SCEP certificate request. Some certificate authorities support a single CN field in the certificate DN, when responding to a SCEP request. When enabled, the CN field contains the value of *certificate name* when you set DN.

### Configuring Revocation

Revocation settings define how and when certificates are revoked. You might want to revoke a certificate that you suspect has been compromised or when a certificate holder leaves a company. You can revoke the certificate manually, or use certificate revocation

list (CRL) or Online Certificate Status Protocol (OCSP) to automatically check for revoked certificates. [Table 69 on page 275](#) describes the revocation settings.

**Table 69: Revocation Settings**

Revocation Settings	Your Action
X.509 Certificate Path Validation Level	<p>X509 contains a specification for a certificate that binds an entity's distinguished name to its public key through the use of a digital signature.</p> <ul style="list-style-type: none"> <li>Full—Use full validation to validate the certificate path back to the root.</li> <li>Partial—Use partial validation to validate the certificate path only part of the way to the root.</li> </ul>
Revocation Check	<p>Select or clear revocation checking for certificates:</p> <ul style="list-style-type: none"> <li>Check for revocation—Select this option to enable revocation checking.</li> <li>Do not check for revocation—Select this option to disable revocation checking.</li> </ul>
Revocation Checking Method	<p>Select the checking method to use if you enabled revocation checking. If you did not enable revocation checking, these fields are unavailable.</p> <ul style="list-style-type: none"> <li>CRL—Enables you to keep a local copy of the revoked certificates on the managed device. This method enables you to check for revoked certificates quickly.</li> <li>OCSP—Enables the device to access a remote OCSP server to check for revoked certificates. Because the OCSP server dynamically updated their list of revoked certificates, this method provides the most up-to-date information.</li> </ul>
Best Effort	<p>Select this option to check for revocation and accept the certificate if no revocation information is found.</p>
CRL Settings	<p>Configure the default setting for the certificate revocation list.</p> <ul style="list-style-type: none"> <li>URL address—Provide the URL address of your internal LDAP server that provides the CRL.</li> <li>LDAP server—Provide the IP address of the external LDAP server that manages the CRL.</li> <li>Refresh Frequency—Select the frequency that the device contacts the CA to obtain a new CRL list: Daily, Weekly, or Monthly.</li> </ul>
OCSP	<p>Enable to dynamically check for revoked certificates.</p> <ul style="list-style-type: none"> <li>Certificate Verification—Select the CA certificate used to verify the signature on the OCSP response.</li> <li>No revoke status check for CA delegated signing cert—Select this option if you do not want the original CA certificate to verify the validity of the CA delegated OCSP signing certificate. When enabled, the validity of the OCSP signing certificate is verified by original CA certificate.</li> <li>URL of OCSP Responder—Provide the URL address of the OCSP server.</li> </ul>

## Configuring Simple Certificate Enrollment Protocol

Alternatively, you can use Simple Certificate Enrollment Protocol (SCEP) to get a local certificate automatically. To enable SCEP for a managed device, configure the default PKI settings for SCEP as described in [Table 70 on page 276](#).

Table 70: Simple Certificate Enrollment Protocol

PKI settings	Your Action
CA CGI	Enter the URL address of the certificate authority certificate generation information.
RA CGI	Enter the URL address of the registration authority certificate generation information that the security device contacts to request a CA certificate.
CA IDENT	Enter the name of the certificate authority to confirm certificate ownership.
Challenge	Enter the challenge word(s) sent to you by the CA that confirm the security device identity to the CA.
CA Certificate Authentication	<p>Configure the default method for obtaining CA certificates:</p> <ul style="list-style-type: none"> <li>• Auto—Select this option for CA certificates retrieved through SCEP.</li> <li>• Manual—Select this option for CA certificates retrieved manually.</li> </ul>
Polling Interval	<p>NSM searches the list of the pending certificates based on this setting and records the time due for the first pending certificate. This process repeats 48 times; after that time, pending certificates can be polled only manually. When polling succeeds, NSM removes the pending certificate from the pending certificate list and schedules no new polling.</p> <ul style="list-style-type: none"> <li>• Poll—When enabled, you can configure the number of minutes between polls.</li> <li>• Do not poll—Use this option to disable automatic polling.</li> </ul>

- Related Documentation**
- [Configuring Certificate Revocation Lists \(NSM Procedure\) on page 273](#)
  - [Certificate Authority Configuration in NSM Overview on page 271](#)



## CHAPTER 9

# Voice Over Internet Protocol

This chapter presents an overview of the Skinny Client Control Protocol (SCCP) Application Layer Gateway (ALG) and lists the firewall security features of the implementation.

This chapter contains the following topics:

- [SCCP Support in ScreenOS Devices Overview on page 277](#)
- [Configuring SCCP ALG in ScreenOS Devices \(NSM Procedure\) on page 278](#)
- [SIP ALG Overview on page 279](#)
- [SIP Request Methods Supported in ScreenOS Devices on page 280](#)
- [Types of SIP Response Classes Supported in ScreenOS Devices on page 282](#)
- [ALG Overview on page 284](#)
- [Configuring SIP ALG in ScreenOS Devices \(NSM Procedure\) on page 285](#)
- [SDP Session Description Overview on page 286](#)
- [Pinhole Creation in ScreenOS Devices Overview on page 287](#)
- [Session Inactivity Timeout in ScreenOS Devices Overview on page 288](#)

### SCCP Support in ScreenOS Devices Overview

---

Skinny Client Control Protocol (SCCP) is supported on security devices in Route, Transparent, and Network Address Translation (NAT) modes. SCCP is a binary-based Application-Layer protocol used for voice over IP (VoIP) call setup and control. In the SCCP architecture, a Cisco H.323 proxy, known as the CallManager, does most of the processing. IP phones, also called end stations, run the Skinny client and connect to a primary (and, if available, a secondary) CallManager over TCP on port 2000 and register with the primary CallManager. This connection is then used to establish calls coming to or from the client.

The SCCP ALG supports the following features:

- **Call flow**—Allows calls from a Skinny client, through the CallManager, to another Skinny client.
- **Seamless failover**—Switches over all calls in process to the standby firewall during failure of the primary firewall.

- VoIP signaling payload inspection—Fully inspects the payload of incoming VoIP signaling packets based on related RFCs and proprietary standards. Any malformed packet attack is blocked by the ALG.
- SCCP signaling payload inspection—Fully inspects the payload of incoming SCCP signaling packets in accordance with RFC 3435. Any malformed-packet attack is blocked by the ALG.
- Stateful processing—Invokes the corresponding VoIP-based state machines to process the parsed information. Any out-of-state or out-of-transaction packet is identified and properly handled.
- Network Address Translation (NAT)—Translates any embedded IP address and port information in the payload, based on the existing routing information and network topology, with the translated IP address and port number, if necessary.
- Pinhole creation and management for VoIP traffic—Identifies IP address and port information used for media or signaling and dynamically opens (and closes) pinholes to securely stream the media.

**Related  
Documentation**

- [SIP ALG Overview on page 279](#)
- [ALG Overview on page 284](#)
- [SDP Session Description Overview on page 286](#)

---

## Configuring SCCP ALG in ScreenOS Devices (NSM Procedure)

---

To configure SCCP ALG:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Select a security device and then double-click the device on which you want to modify the ALG section. The device configuration appears.
3. In the device navigation tree, select **Advanced > ALGs**.
4. Select **Enable SCCP ALG**.
5. Click the **Show** button to expand the SIP settings.
6. Use the Up or Down arrow keys to specify the inactive media timeout. The default setting is 120 seconds.
7. Select the **Enable Call Flood Protection to Call Manager** check box. The feature is not enabled by default.
8. Enter a threshold value for the maximum number of calls per minute. The default is 20 calls per minute.



**NOTE:** The threshold value is per client to protect the CallManager from being flooded with new calls either by an already compromised connected client or a faulty device.

---

9. Select **Pass unidentified Skinny message in Route mode** check box.
10. Select **Pass unidentified Skinny message in NAT mode** check box.



**NOTE:** When you select the “pass unidentified message” option in either Route or NAT mode, the message that had an error in decoding (because of unidentified message ID or parameter) is forwarded as-is without any processing.

11. Click **OK** to apply your settings.

#### Related Documentation

- [SCCP Support in ScreenOS Devices Overview on page 277](#)
- [SIP ALG Overview on page 279](#)
- [ALG Overview on page 284](#)
- [SDP Session Description Overview on page 286](#)
- 

## SIP ALG Overview

Session Initiation Protocol (SIP) is an Internet Engineering Task Force (IETF) 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.

Juniper Networks security devices support SIP as a service and can screen SIP traffic, allowing and denying it based on a policy that you configure. SIP is a predefined service in ScreenOS and uses port 5060 as the destination port.

SIP's primary function is to distribute session-description information and, during the session, to negotiate and modify the parameters of the session. SIP is also used to terminate a multimedia session.

Session-description information is included in INVITE and ACK messages and indicates the multimedia type of the session, for example, voice or video. Although SIP can use different description protocols to describe the session, the Juniper Networks SIP ALG supports only Session Description Protocol (SDP).

SDP provides information that a system can use to join a multimedia session. SDP might include information such as IP addresses, port numbers, times, and dates. Note that the IP address and port number in the SDP header (the “c=” and “m=” fields, respectively) are the address and port where the client wants to receive the media streams and not the IP address and port number from which the SIP request originates (although they can be the same). See “[SDP Session Description Overview](#)” on page 286 for more information.

SIP messages consist of requests from a client to a server and responses to the requests from a server to a client with the purpose of establishing a session (or a call). A User

Agent (UA) is an application that runs at the endpoints of the call and consists of two parts: the User Agent Client (UAC), which sends SIP requests on behalf of the user; and a User Agent Server (UAS), which listens to the responses and notifies the user when they arrive. Examples of UAs are SIP proxy servers and phones.

**Related Documentation**

- [SCCP Support in ScreenOS Devices Overview on page 277](#)
- [ALG Overview on page 284](#)
- [SIP Request Methods Supported in ScreenOS Devices on page 280](#)
- [Types of SIP Response Classes Supported in ScreenOS Devices on page 282](#)

## SIP Request Methods Supported in ScreenOS Devices

The SIP transaction model includes a number of request and response messages, each of which contains a *method* field that denotes the purpose of the message. The method types and response codes supported by ScreenOS are listed in [Table 71 on page 280](#).

**Table 71: SIP Request Methods**

Method Types/Response Codes	Description	Modified Fields
INVITE	A user sends an INVITE request to invite another user to participate in a session. The body of an INVITE request may contain the description of the session.	In NAT mode, the IP addresses in the Via, From, To, Call-ID, Contact, Route, and Record-Route header fields are modified.
ACK	The user from whom the INVITE originated sends an ACK request to confirm reception of the final response to the INVITE request. If the original INVITE request did not contain the session description, the ACK request must include it.	In NAT mode, the IP addresses in the Via, From, To, Call-ID, Contact, Route, and Record-Route header fields are modified.
OPTIONS	A User Agent (UA) uses OPTIONS to obtain information about the capabilities of the SIP proxy. A server responds with information about what methods, session description protocols, and message encoding it supports. In NAT mode, when the OPTIONS request is sent from a UA outside NAT to a proxy inside NAT, the SIP ALG translates the address in the Request-URI and the IP address in the To field to the appropriate IP address of the internal client. When the UA is inside NAT and the proxy is outside NAT, the SIP ALG translates the From, Via, and Call-ID fields.	NA

Table 71: SIP Request Methods (*continued*)

Method Types/Response Codes	Description	Modified Fields
BYE	A user sends a BYE request to abandon a session. A BYE request from either user automatically terminates the session.	In NAT mode, the IP addresses in the Via, From, To, Call-ID, Contact, Route, and Record-Route header fields are modified.
CANCEL	A user sends a CANCEL request to cancel a pending INVITE request. A CANCEL request has no effect if the SIP server processing the INVITE had sent a final response for the INVITE before it received the CANCEL.	In NAT mode, the IP addresses in the Via, From, To, Call-ID, Contact, Route, and Record-Route header fields are modified.
REGISTER	A user sends a REGISTER request to a SIP registrar server to inform it of the current location of the user. A SIP registrar server records all the information it receives in REGISTER requests and makes this information available to any SIP server attempting to locate a user.	<p>In NAT mode, REGISTER requests are handled as follows:</p> <ul style="list-style-type: none"> <li>REGISTER requests from an external client to an internal registrar—When the SIP ALG receives the incoming REGISTER request it translates the IP address, if any, in the Request-URI. Incoming REGISTER messages are allowed only to a MIP or VIP address. No translation is needed for the outgoing response.</li> <li>REGISTER requests from an internal client to an external registrar—When the SIP ALG receives the outgoing REGISTER request it translates the IP addresses in the To, From, Via, Call-ID, and Contact: header fields. A backward translation is performed for the incoming response.</li> </ul>
Info	Used to communicate mid-session signaling information along the signaling path for the call.	In NAT mode, the IP addresses in the Via, From, To, Call-ID, Contact, Route, and Record-Route header fields are modified.
Subscribe	Used to request current state and state updates from a remote node. In NAT mode, the address in the Request-URI is changed to a private IP address if the message is coming from the external network into the internal network.	The IP addresses in Via, From, To, Call-ID, Contact, Route, and Record-Route header fields are modified.

Table 71: SIP Request Methods (*continued*)

Method Types/Response Codes	Description	Modified Fields
Notify	Sent to inform subscribers of changes in state to which the subscriber has a subscription. In NAT mode, the IP address in the Request-URL header field is changed to a private IP address if the message is coming from the external network into the internal network.	The IP address in the Via, From, To, Call-ID, Contact, Route, and Record-Route header fields are modified.
Refer	Used to refer the recipient (identified by the Request-URI) to a third party by the contact information provided in the request.	<p>In NAT mode, the IP address in the Request-URI is changed to a private IP address if the message is coming from the external network into the internal network. The IP addresses in the Via, From, To, Call-ID, Contact, Route, and Record-Route header fields are modified.</p> <p>For example, if user A in a private network refers user B in a public network to user C, who is also in the private network, the SIP ALG allocates a new IP address and port number for user C so that user C can be contacted by user B. If user C is registered with a registrar, however, its port mapping is stored in the ALG NAT table and is reused to perform the translation.</p>
Update	Used to open pinhole for new or updated SDP information	The Via, From, To, Call-ID, Contact, Route, and Record-Route header fields are modified.
1xx, 202, 2xx, 3xx, 4xx, 5xx, 6xx Response Codes	Used to indicate the status of a transaction.	

**Related  
Documentation**

- [SCCP Support in ScreenOS Devices Overview on page 277](#)
- [ALG Overview on page 284](#)
- [Types of SIP Response Classes Supported in ScreenOS Devices on page 282](#)

## Types of SIP Response Classes Supported in ScreenOS Devices

SIP responses provide status information about SIP transactions and include a response code and a reason phrase. SIP responses are grouped into the following classes:

- Informational (100 to 199)—Request received, continuing to process the request.
- Success (200 to 299)—Action successfully received, understood, and accepted.
- Redirection (300 to 399)—Further action required to complete the request.
- Client Error (400 to 499)—Request contains bad syntax or cannot be fulfilled at this server.
- Server Error (500 to 599)—Server failed to fulfill an apparently valid request.
- Global Failure (600 to 699)—Request cannot be fulfilled at any server.

Table 72 on page 283 provides a complete list of current SIP responses, all of which are supported on Juniper Networks security devices.

**Table 72: SIP Responses**

Class	Response Code-Reason Phrase	Response Code-Reason Phrase	Response Code-Reason Phrase
Informational	100 Trying	180 Ringing	181 Call is being forwarded
	182 Queued	183 Session progress	
Success	200 OK	202 Accepted	
Redirection	300 Multiple choices	301 Moved permanently	302 Moved temporarily
	305 Use proxy	380 Alternative service	
Client Error	400 Bad request	401 Unauthorized	402 Payment required
	403 Forbidden	404 Not found	405 Method not allowed
	406 Not acceptable	407 Proxy authentication required	408 Request time-out
	409 Conflict	410 Gone	411 Length required
	413 Request entity too large	414 Request-URL too large	415 Unsupported media type
	420 Bad extension	480 Temporarily not available	481 Call leg/transaction does not exist
	482 Loop detected	483 Too many hops	484 Address incomplete
	485 Ambiguous	486 Busy here	487 Request canceled
	488 Not acceptable here		
Server Error	500 Server internal error	501 Not implemented	502 Bad gateway
	502 Service unavailable	504 Gateway time-out	505 SIP version not supported

Table 72: SIP Responses (*continued*)

Class	Response Code-Reason Phrase	Response Code-Reason Phrase	Response Code-Reason Phrase
Global Failure	600 Busy everywhere	603 Decline	604 Does not exist anywhere
	606 Not acceptable		

**Related Documentation**

- [SCCP Support in ScreenOS Devices Overview on page 277](#)
- [SIP ALG Overview on page 279](#)
- [SIP Request Methods Supported in ScreenOS Devices on page 280](#)
- [ALG Overview on page 284](#)
- [SDP Session Description Overview on page 286](#)

## ALG Overview

There are two types of SIP traffic, the signaling and the media stream. SIP signaling traffic consists of request and response messages between client and server and uses transport protocols such as User Datagram Protocol (UDP) or Transmission Control Protocol (TCP). The media stream carries the data (audio data, for example) and uses Application Layer protocols such as Real-Time Transport Protocol (RTP) over UDP.

Juniper Networks security devices support SIP signaling messages on port 5060. You can simply create a policy that permits SIP service, and the security device filters SIP signaling traffic like any other type of traffic, permitting or denying it. The media stream, however, uses dynamically assigned port numbers that can change several times during the course of a call. Without fixed ports, it is impossible to create a static policy to control media traffic. In this case, the security device invokes the SIP ALG. The SIP ALG reads SIP messages and their SDP content and extracts the port-number information it needs to dynamically open pinholes and let the media stream traverse the security device.



**NOTE:** We refer to a pinhole as the limited opening of a port to allow exclusive traffic.

The SIP ALG monitors SIP transactions and dynamically creates and manages pinholes based on the information it extracts from these transactions. The Juniper Networks SIP ALG supports all SIP methods and responses (see [“SIP Request Methods Supported in ScreenOS Devices” on page 280](#) and [“Types of SIP Response Classes Supported in ScreenOS Devices” on page 282](#)). You can allow SIP transactions to traverse the Juniper Networks firewall by creating a static policy that permits SIP service. This policy enables the security device to intercept SIP traffic and do one of the following actions: permit or deny the traffic or enable the SIP ALG to open pinholes to pass the media stream. The SIP ALG needs to open pinholes only for the SIP requests and responses that contain



media information (that is, SDP). For SIP messages that do not contain SDP, the security device simply lets them through.

The SIP ALG intercepts SIP messages that contain SDP and, using a parser, extracts the information it requires to create pinholes. The SIP ALG examines the SDP portion of the packet, and a parser extracts information such as IP addresses and port numbers, which the SIP ALG records in a pinhole table. The SIP ALG uses the IP addresses and port numbers recorded in the pinhole table to open pinholes and allow media streams to traverse the security device.



**NOTE:** Juniper Networks security devices do not support encrypted SDP. If a security device receives a SIP message in which SDP is encrypted, the SIP ALG permits it through the firewall but generates a log message informing the user that it cannot process the packet. If SDP is encrypted, the SIP ALG cannot extract the information it needs from SDP to open pinholes. As a result, the media content that SDP describes cannot traverse the security device.

**Related  
Documentation**

- [SCCP Support in ScreenOS Devices Overview on page 277](#)
- [SIP ALG Overview on page 279](#)
- [SDP Session Description Overview on page 286](#)

## Configuring SIP ALG in ScreenOS Devices (NSM Procedure)

To configure SIP ALG:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Select a security device and then double-click the device on which you want to modify the ALG section. The device configuration appears.
3. In the navigation tree, select **Advanced > ALGs**.
4. Select **Enable SIP ALG**.
5. Click the **Show** button to expand the SIP settings.
6. Use the Up or Down Arrow keys to configure the following:
  - Signaling Inactivity Timeout—The default setting is 43,200 seconds (12 hours).
  - Media Inactivity Timeout—The default setting is 120 seconds.
  - Maximum duration a message will remain in network—The default setting is 5 seconds.
  - Round Trip Time Estimate—The default setting is 500 milliseconds.
  - Invite Transaction Timeout—The default setting is 3 minutes.

7. Select **IP Attack Protection** and specify a Timeout if you want IP attack protection to be enabled.
8. Click **OK** to apply your settings.

**Related Documentation**

- [SIP ALG Overview on page 279](#)
- [SIP Request Methods Supported in ScreenOS Devices on page 280](#)
- [Types of SIP Response Classes Supported in ScreenOS Devices on page 282](#)
- [ALG Overview on page 284](#)
- [SDP Session Description Overview on page 286](#)

## SDP Session Description Overview

An SDP session description is text-based and consists of a set of lines. It can contain session-level and media-level information. The session-level information applies to the whole session, while the media-level information applies to a particular media stream. An SDP session description always contains session-level information, which appears at the beginning of the description, and might contain media-level information, which comes after.



**NOTE:** In the SDP session description, the media-level information begins with the **m=** field.

Of the many fields in the SDP session description, two are particularly useful to the SIP ALG because they contain Transport Layer information. The two fields are the following:

SDP	SDP Format	Description
<b>c=</b> for connection information	This field can appear at the session or media level. It displays in this format:  c=<network type><address type><connection address>	Currently, the security device supports only "IN" (for Internet) as the network type, "IP4" as the address type, and a unicast IP address or domain name as the destination (connection) IP address.  <b>NOTE:</b> Generally, the destination IP address can also be a multicast IP address, but ScreenOS does not currently support multicast with SIP.
<b>m=</b> for media announcement	This field appears at the media level and contains the description of the media. It displays in this format:  m=<media><port><transport><fmt list>	Currently, the security device supports only "audio" as the media and "RTP" as the Application Layer transport protocol. The port number indicates the destination (not the origin) of the media stream. The format list (fmt list) provides information on the Application Layer protocol that the media uses.

- If the destination IP address is a unicast IP address, the SIP ALG creates pinholes using the IP address and port numbers specified in the media description field **m=**.

In this release of ScreenOS, the security device opens ports only for RTP and Real-Time Control Protocol (RTCP). Every RTP session has a corresponding RTCP session.

Therefore, whenever a media stream uses RTP, the SIP ALG must reserve ports (create pinholes) for both RTP and RTCP traffic. By default, the port number for RTCP is one higher than the RTP port number.

- In this configuration, the following connections are logged:
  - Any connections into eth4 from any IP address except the database server IP address are logged with an alert.
  - Any connections into eth2 from any IP address except the Web server are logged. In addition, if the database server IP address appears in eth2, the sensor logs that event.

#### Related Documentation

- [SCCP Support in ScreenOS Devices Overview on page 277](#)
- [SIP ALG Overview on page 279](#)
- [ALG Overview on page 284](#)

## Pinhole Creation in ScreenOS Devices Overview

Both pinholes for the RTP and RTCP traffic share the same destination IP address. The IP address comes from the c= field in the SDP session description. Because the c= field can appear in either the session-level or media-level portion of the SDP session description, the parser determines the IP address based on the following rules (in accordance with SDP conventions):

- First, the SIP ALG parser verifies if there is a c= field containing an IP address in the media level. If there is one, the parser extracts that IP address, and the SIP ALG uses it to create a pinhole for the media.
- If there is no c= field in the media level, the SIP ALG parser extracts the IP address from the c= field in the session level, and the SIP ALG uses it to create a pinhole for the media. If the session description does not contain a c= field in either level, this indicates an error in the protocol stack, and the security device drops the packet and logs the event.

[Table 73 on page 287](#) displays the information the SIP ALG needs to create a pinhole. This information comes from the SDP session description and parameters on the security device:

**Table 73: Information for Pinhole Creation**

Field	Description
Protocol	UDP.
Source IP	Unknown.
Source port	Unknown.
Destination IP	The parser extracts the destination IP address from the c= field in the media or session level.

Table 73: Information for Pinhole Creation (*continued*)

Field	Description
Destination port	The parser extracts the destination port number for RTP from the m= field in the media level and calculates the destination port number for RTCP using the following formula:  RTP port number + one
Lifetime	This value indicates the length of time (in seconds) during which a pinhole is open to allow a packet through. A packet must go through the pinhole before the lifetime expires. When the lifetime expires, the SIP ALG removes the pinhole. When a packet goes through the pinhole within the lifetime period, immediately afterwards the SIP ALG removes the pinhole for the direction from which the packet came.

- Related Documentation**
- [SIP ALG Overview on page 279](#)
  - [ALG Overview on page 284](#)
  - [Session Inactivity Timeout in ScreenOS Devices Overview on page 288](#)

## Session Inactivity Timeout in ScreenOS Devices Overview

Typically a call ends when one of the clients sends a BYE or CANCEL request. The SIP ALG intercepts the BYE or CANCEL request and removes all media sessions for that call. There could be reasons or problems preventing clients in a call from sending BYE or CANCEL requests, for example, a power failure. In this case, the call might go on indefinitely, consuming resources on the security device. The inactivity-timeout feature helps the security device to monitor the liveliness of the call and terminate it if there is no activity for a specific period of time.

A call can have one or more voice channels. Each voice channel has two sessions (or two media streams), one for RTP and one for RTCP. When managing the sessions, the security device considers the sessions in each voice channel as one group. Settings such as the inactivity timeout apply to a group as opposed to each session.

- **Signaling-inactivity timeout**— This parameter indicates the maximum length of time (in seconds) a call can remain active without any SIP-signaling traffic. Each time a SIP-signaling message occurs within a call, this timeout resets. The default setting is 43,200 seconds (12 hours).
- **Media-inactivity timeout**— This parameter indicates the maximum length of time (in seconds) a call can remain active without any media (RTP or RTCP) traffic within a group. Each time an RTP or RTCP packet occurs within a call, this timeout resets. The default setting is 120 seconds.

If either of these timeouts expires, the security device removes all sessions for this call from its table, thus terminating the call.

- Related Documentation**
- [SIP ALG Overview on page 279](#)
  - [SIP Request Methods Supported in ScreenOS Devices on page 280](#)

- [Types of SIP Response Classes Supported in ScreenOS Devices on page 282](#)
- [ALG Overview on page 284](#)



## CHAPTER 10

# Routing

This chapter provides information on using the Virtual Router screens to configure routing on security devices. Routing is the process of forwarding packets from one network to another toward a final destination, and a router is a point where one network meets another network. Security devices contain integrated routing functionality that enables them to effectively forward protected traffic to its destination.

This chapter contains the following topics:

- [Configuring Virtual Routers on page 292](#)
- [Route Types Overview on page 293](#)
- [Virtual Routers Overview on page 294](#)
- [Configuring Virtual Routers \(NSM Procedure\) on page 294](#)
- [Virtual Router General Properties Overview on page 295](#)
- [Access List Overview on page 296](#)
- [Example: Configuring Access Lists \(NSM Procedure\) on page 297](#)
- [Route Map Overview on page 298](#)
- [Export and Import Rules in a Virtual Router Overview on page 300](#)
- [Example: Configuring Export Rules in a Virtual Router \(NSM Procedure\) on page 301](#)
- [Routing Table Entries Overview on page 303](#)
- [Destination-Based Routes Overview on page 305](#)
- [Source-Based Routes Overview on page 306](#)
- [Example: Configuring Source-Based Routes \(NSM Procedure\) on page 306](#)
- [Source Interface-Based Routes Overview on page 307](#)
- [Example: Source-Interface-Based Routing \(NSM Procedure\) on page 308](#)
- [Configuring Route Preferences on page 310](#)
- [Dynamic Routing Configuration Overview on page 311](#)
- [OSPF Protocol Configuration Overview on page 311](#)
- [Enabling OSPF \(NSM Procedure\) on page 312](#)
- [Global OSPF Settings Overview on page 313](#)
- [Configuring OSPF Interface Parameters Overview on page 315](#)

- [Configuring OSPF \(NSM Procedure\) on page 318](#)
- [RIP Overview on page 319](#)
- [Configuring RIP \(NSM Procedure\) on page 320](#)
- [Global RIP Settings Overview on page 321](#)
- [RIP Interface Parameters Overview on page 323](#)
- [BGP Overview on page 325](#)
- [Route-Refresh Capabilities Overview on page 326](#)
- [Configuring BGP Networks on page 327](#)
- [Configuring Aggregate Addresses on page 327](#)
- [Configuring Neighbors and Peer Groups Overview on page 328](#)
- [Configuring a BGP Routing Instance \(NSM Procedure\) on page 329](#)
- [Configuring NHRP Overview on page 330](#)
- [Configuring OSPFv3 Overview on page 331](#)
- [Configuring RIPng Overview on page 334](#)
- [Multicast Route Overview on page 335](#)
- [Configuring IGMP \(NSM Procedure\) on page 336](#)
- [Configuring IGMP Proxy \(NSM Procedure\) on page 337](#)
- [Configuring PIM Sparse Mode \(NSM Procedure\) on page 339](#)
- [Configuring a Rendezvous Point to Group Mappings \(NSM Procedure\) on page 340](#)
- [Configuring Acceptable Groups \(NSM Procedure\) on page 341](#)
- [Example: Configuring Proxy RP on page 342](#)
- [Multicast Routing Table Entries Overview on page 344](#)
- [Multicast Routing Table Preferences Overview on page 344](#)
- [Configuring Multicast Static Routes on page 345](#)
- [Example: Configuring Multicast Static Routes \(NSM Procedure\) on page 345](#)
- [IRDP Support Overview on page 346](#)
- [Example: Configuring ICMP Router Discovery Protocol \(NSM Procedure\) on page 347](#)
- [Disabling IRDP on page 348](#)
- [Policy-Based Routing Overview on page 349](#)
- [Example: Configuring Policy-Based Routing \(NSM Procedure\) on page 349](#)

---

## Configuring Virtual Routers

To configure a virtual router, double-click the virtual router in the Virtual Router configuration screen (or, either select the virtual router and then click the Edit icon, or right-click the virtual router and select **Edit**). You can configure the following parameters for a virtual router:



- Virtual router general properties
- Access lists
- Route Maps
- Export and import rules
- Routing table entries
- Route preferences

For details on configuring dynamic routing protocols (BGP, RIP, OSPF) in the virtual router and on the interfaces, see [“Dynamic Routing Configuration Overview” on page 311](#). For details on configuring multicast routing protocols (PIM-SIM, IGMP, IGMP-Proxy) and multicast route entries, see [“Multicast Route Overview” on page 335](#).

For more detailed explanations about virtual routers and dynamic routing protocols on security devices, see the *Concepts & Examples ScreenOS Reference Guide: Dynamic Routing*.

#### Related Documentation

- [Route Types Overview on page 293](#)
- [Virtual Routers Overview on page 294](#)
- [Virtual Router General Properties Overview on page 295](#)
- [Route Map Overview on page 298](#)

## Route Types Overview

You can configure three types of routing on a security device:

- **Static**—Static routes are mappings of IP network addresses to next-hop destinations that you define on a Layer 3 forwarding device, such as a router. These mappings do not change unless you alter them. For networks that have few connections to other networks or where internetwork connections are relatively unchanging, it is usually more efficient to define static routes than to set up dynamic routing. The device retains static routes until you explicitly remove them. However, you can override static routes with dynamic routing information if necessary.
- **Dynamic**—Dynamic routing involves routers exchanging information about the reachability of networks and subnetworks and adjusting routing tables by analyzing incoming routing update messages. These messages populate the network, directing routers to recalculate routes and change their routing tables accordingly.
- **Multicast**—Multicast protocols enable routers to forward traffic from one source to multiple receivers simultaneously.

All routes are contained within a virtual router.

#### Related Documentation

- [Configuring Virtual Routers on page 292](#)
- [Virtual Routers Overview on page 294](#)
- [Virtual Router General Properties Overview on page 295](#)

- [Route Map Overview on page 298](#)

## Virtual Routers Overview

---

A security device can divide its routing component into two or more virtual routers. A virtual router supports static routing, dynamic routing protocols, and multicast protocols, which you can enable simultaneously in one virtual router. A security device can contain the following types of virtual routers (VRs):

- **Predefined Virtual Routers**—Each security device contains two predefined virtual routers:
  - **trust-vr**—By default, contains all predefined security zones and any user-defined zones.
  - **untrust-vr**—By default, does not contain any security zones.

You cannot delete the trust-vr or untrust-vr predefined virtual routers.

- **Custom Virtual Routers**—On some security devices, you can create and configure additional custom virtual routers.

You can define multiple VRs, but trust-vr is the default VR. All predefined and custom security zones (and all interfaces bound to those security zones) are bound to the trust-vr virtual router. To bind a security zone to the untrust-vr or to a custom VR, you must first unbind all interfaces from the zone. For a virtual system (vsys), you can select a virtual router to be the default router for the vsys.

The management virtual router supports out-of-band management and segregates firewall management traffic away from production traffic. The feature is disabled by default and you can enable it by setting a virtual router.

### Related Documentation

- [Configuring Virtual Routers on page 292](#)
- [Route Types Overview on page 293](#)
- [Virtual Router General Properties Overview on page 295](#)
- [Route Map Overview on page 298](#)

## Configuring Virtual Routers (NSM Procedure)

---

To configure an ISG2000 device running ScreenOS 6.2 or later:

1. In the NSM navigation tree, select **Device Manager > Devices**. Double-click the device object to open the device configuration.
2. Click the **Edit** icon to edit the ISG2000 device.
3. In the device navigation tree, click **Network > Virtual Router**. The Virtual Router screen appears.
4. Create a customer virtual router, customer-vr1, and save the changes.

5. Select **customer-vr1** from the Management Vrouter drop-down list.
6. Create a customer zone, customer-zone1, or edit any existing one by clicking **Network > Zone**.
7. Select **Virtual Router** for customer-zone1.
8. Edit the management interface by clicking **Network > Interface**.
9. Select **Zone** for customer-zone1.
10. Click **OK** to save the changes.

**Related  
Documentation**

- [Route Types Overview on page 293](#)
- [Virtual Router General Properties Overview on page 295](#)
- [Route Map Overview on page 298](#)

## Virtual Router General Properties Overview

The general properties for a virtual router that can be configured are displayed in [Table 74 on page 295](#):

**Table 74: Virtual Router General Properties**

Property	Description
Virtual Router ID	A unique identifier used to communicate with other routing devices. The identifier can be in the form of a dotted decimal notation, like an IP address, or an integer value. If you do not configure a specific virtual router ID before enabling a dynamic routing protocol, the device automatically selects the highest IP address of the active interfaces in the VR for the router identifier.
Maximum Number of Routes	The maximum number of routing table entries that can be allocated for a specific virtual router. The maximum number of route entries available depends upon the security device and the number of virtual routers configured on the device. Setting the maximum number of route entries in a VR helps prevent one virtual router from using up all the entries in the system.
Maximum Equal Cost Routes Supported (ScreenOS 5.1 and later only)	The maximum equal cost multi-path (ECMP) routes used by the virtual router. You might want to use ECMP when load balancing to enable the route lookup to select a different route each time the route is invoked. This setting controls how many ECMP routes the route lookup can use; you can configure one to four ECMP routes for each virtual router. For example, when this setting is three and the number of available ECMP routes is five, the route lookup uses only the first three ECMP entries in the routing table (in roundsrobin fashion) for the virtual router.
Route Lookup Preference (ScreenOS 5.1 and later only)	Configure the order in which route lookup occurs. By default, route lookup uses the following sequence: SIBR routes (preferred value 3), source-based routes (preferred value 2), destination-based routes (preferred value 1). To change this sequence, configure the values for each preference from 1 to 255; the higher the value, the more preferred the route.

**Table 74: Virtual Router General Properties (*continued*)**

Property	Description
Shared VR	You can make the VR accessible from any virtual system (vsys) on the device. By default, only the untrust-vr is a shared VR that is accessible by any vsys. You can configure other root-level VRs to be sharable.
Route Exporting	(For the trust-vr only) You can enable or disable automatic route exporting to the untrust-vr for interfaces configured in Route mode.
Consider Active Routes	You can direct the virtual router to consider active routes on inactive interfaces for redistribution or export. By default, only active routes defined on active interfaces can be redistributed to other protocols or exported to other virtual routers.
SNMP Private Traps	You can specify the use of SNMP private traps for managing virtual router objects, including objects in the dynamic routing MIB. This option is only available for the default root-level virtual router.
Ignore Overlapping Subnets	You can direct the virtual router to ignore overlapping subnet addresses for interfaces in the virtual router. By default, you cannot configure overlapping subnet IP addresses on interfaces in the same virtual router.
Next Hop	(For the trust-vr only) You can direct the virtual router to use the untrust-vr as the next hop for the default route.

For instructions for configuring virtual router general properties, see the *Network and Manager Security Manager Online Help*.

#### Related Documentation

- [Configuring Virtual Routers on page 292](#)
- [Route Types Overview on page 293](#)
- [Virtual Routers Overview on page 294](#)
- [Access List Overview on page 296](#)

## Access List Overview

An access list is a sequential list of statements against which a route is compared. Each entry in the list specifies the IP address or netmask of a network prefix and the forwarding status (whether to permit or deny the route).

For example, an entry in an access list can permit routes for the 1.1.1.0/24 subnetwork, while another entry in the same access list can deny routes for the 2.2.2.0/24 subnetwork. If a route matches an entry in the access list, the specified forwarding status is applied. If the two entries are in an access list, a route to the host at 1.1.1.10 is permitted, while the route to the host at 2.2.2.10 is denied.

You can also use access lists to control the flow of multicast control traffic. You can create an access list to restrict the multicast groups that hosts can join or the sources

from which multicast traffic is received. After you create an access list, you can include it in a multicast rule.

The sequence of entries in an access list is important. A route is first compared to the entry in the access list with the lowest sequence number and then to other entries in ascending sequence number until there is a match. If there is a match, all subsequent entries in the access list are ignored. Therefore, you should sequence the more specific entries before less specific entries. For example, place the entry that denies routes for the 1.1.1.1/30 subnetwork before the entry that permits routes for the 1.1.1.0/24 subnetwork. On devices running ScreenOS 6.3, access list supports IPv6.

For instructions for configuring virtual router access lists, see the *Network and Security Manager Online Help*.

#### Related Documentation

- [Configuring Virtual Routers on page 292](#)
- [Route Types Overview on page 293](#)
- [Virtual Routers Overview on page 294](#)
- [Virtual Router General Properties Overview on page 295](#)
- [Example: Configuring Access Lists \(NSM Procedure\) on page 297](#)

### Example: Configuring Access Lists (NSM Procedure)

In this example, you create an access list on the trust-vr.

To create an access list on the trust-vr:

1. In the NSM navigation tree, select **Device Manager > Devices**. Double-click the device object to open the device configuration.
2. In the device navigation tree, select **Network > Virtual Routers**.
3. Double-click the trust-vr virtual router. The General Properties screen appears.
4. In the virtual router navigation tree, select **Access List**, and then click the Add icon in the main display area. The Access List Entries/New dialog box appears.
5. For Access List Number, enter **2**. This number uniquely identifies the access list.
6. In the Access List Entries area, click the Add icon. The New Access List Entry dialog box appears. Configure the following:
  - For Sequence Number, enter **10**. This number positions this statement relative to other statements in the access list.
  - For Action, select **Permit**.
  - For Prefix, select **Prefix to Filter** and enter the IP address/netmask **1.1.1.1/24**.
7. Click **OK** to save the new access list.
8. Click **OK** to save your changes to the virtual router, and then click **OK** again to save your changes to the device configuration.

**Related Documentation**

- [Configuring Virtual Routers on page 292](#)
- [Route Types Overview on page 293](#)
- [Virtual Routers Overview on page 294](#)
- [Virtual Router General Properties Overview on page 295](#)
- [Access List Overview on page 296](#)
- [Route Map Overview on page 298](#)

## Route Map Overview

A *route map* is a set of statements that the device applies in sequential order to a route. Each statement in the route map defines a condition that is compared to the route. A route is compared to each statement in a specified route map in order of increasing sequence number until there is a match, then the action specified by the statement is applied. If the route matches the condition in the route map statement, the route is either permitted or rejected.

A route map statement can also modify certain attributes of a matching route. There is an implicit deny at the end of every route map; that is, if a route does not match any entry in the route map, the route is rejected.

For each match condition, you specify whether a route that matches the condition is accepted (permitted) or rejected (denied). If a route matches a condition and is permitted, you can optionally set attribute values for the route. You can configure additional entries for the same route map, specifying a different sequence number for each entry.

### Route Map Match Conditions

The match conditions that can be configured for a route map are displayed in [Table 75 on page 298](#).

**Table 75: Route MAP Match Conditions**

Property	Description
AS Path (BGP)	Select the AS path access list a route must match.
Community (BGP)	Select the community a route must match.
Metric	Select the route metric a route must match.
Interface	Select the interfaces a route must match.
Access List	Select the access list a route must match.
Next-Hop	Match a specified access list. It also supports IPv6, from ScreenOS 6.3.

**Table 75: Route MAP Match Conditions (*continued*)**

Property	Description
Route Type (OSPF)	Select the route types (OSPF internal, external type 1, or external type 2) that a route must match.
Tag	Select the route tag value a route must match.

**Permitted Route Attributes**

The attributes that be configured for matching permitted routes are displayed in [Table 76 on page 299](#).

**Table 76: Permitted Route Attributes**

Property	Description
AS Path (BGP)	Prepends a specified AS path access list to the path list attribute of the matching route.
Community (BGP)	Sets the community attribute of the matching route to the specified community list.
Next-Hop	Sets the next-hop of the matching route to the specified IP address.
Tag	Sets the tag of the matching route to the specified tag value or IP address.
Weight	Sets the weight of the matching route.
Metric Type (OSPF)	Sets the OSPF metric type of the matching route to either external type 1 or external type 2.
Local Preference (BGP)	Sets the local-pref attribute of the matching route to the specified value.
Preserve preference (ScreenOS 5.1 and later only)	Preserves the preference value of the matching route that is exported into another virtual router.

Table 76: Permitted Route Attributes (*continued*)

Property	Description
Metric	<p>Configures how the virtual router assigns a metric to permitted routes (select one):</p> <ul style="list-style-type: none"> <li>• Use Metric Specified By User as Imported/Exported Route Metric—When enabled, the VR assigns the specified metric value to all matching routes.</li> <li>• Use the Source Route Metric as the Imported/Exported Route Metric—When enabled, the VR preserves the metric of a matching route that is imported or exported into another virtual router.</li> <li>• Offset Metric (ScreenOS 5.1 and higher only)—When enabled, the VR increments the metric of the matching route by the specified number. Use this option to increase the metric on a less desirable path. For RIP routes, you can apply the increment to either routes advertised (route-map out) or routes learned (route-map in). For other routes, you can apply the increment to routes that are exported into another virtual router.</li> </ul>

For instructions on configuring virtual router route maps, see the *Network and Security Manager Online Help*.

#### Related Documentation

- [Configuring Virtual Routers on page 292](#)
- [Route Types Overview on page 293](#)
- [Virtual Routers Overview on page 294](#)
- [Virtual Router General Properties Overview on page 295](#)
- [Access List Overview on page 296](#)
- [Export and Import Rules in a Virtual Router Overview on page 300](#)
- [Routing Table Entries Overview on page 303](#)

## Export and Import Rules in a Virtual Router Overview

When the security device has multiple virtual routers, you can enable one VR to learn specified routes in another VR.

- Use an *export rule* on the source VR to export specific routes to the destination VR. When exporting routes, a virtual router permits other VRs to learn about its network.
- Use an *import rule* on the destination VR to import specific routes from the source VR. Import rules control which routes can be imported; if the destination VR does not contain any import rules, the destination VR accepts all exported routes, however, if you create an import rule, the destination VR accepts only the routes specified in the import rule.

Configuring an export or import rule is similar to configuring a redistribution rule. You configure a *route map* to specify which routes are to be exported/imported and the attributes of the routes.



You can also configure the trust-vr to automatically export all its route table entries to the untrust-vr, or configure a user-defined virtual router to automatically export routes to other virtual routers. However, this does not necessarily mean that the untrust-vr imports all the routes exported by the trust-vr. If you define import rules for the untrust-vr, only routes that match the import rules are imported.

From ScreenOS 6.3, security devices also support OSPFv3 protocols while importing or exporting rules in a VR.

For instructions on configuring virtual router export and import rules, see the *Network and Security Manager Online Help*.

#### Related Documentation

- [Configuring Virtual Routers on page 292](#)
- [Virtual Routers Overview on page 294](#)
- [Virtual Router General Properties Overview on page 295](#)
- [Access List Overview on page 296](#)
- [Route Map Overview on page 298](#)
- [Example: Configuring Export Rules in a Virtual Router \(NSM Procedure\) on page 301](#)

### Example: Configuring Export Rules in a Virtual Router (NSM Procedure)

In this example, you export OSPF routes for the 1.1.1.1/24 network in the trust-vr virtual router to the untrust-vr routing domain. You first create an access list for the network prefix 1.1.1.1/24, which is then used in the route map "rtmap1" to filter for matches of routes for the 1.1.1.1/24 network. You then create a route export rule to export matching OSPF routes from the trust-vr to the untrust-vr virtual router.

To configure export rules in a virtual router:

1. In the NSM navigation tree, select **Device Manager > Devices**. Double-click the device object to open the device configuration.
2. In the device navigation tree, select **Network > Virtual Routers**.
3. Double-click the trust-vr virtual router. The General Properties screen appears.
4. Configure the access list:
  - In the virtual router navigation tree, select **Access List**, then click the Add icon in the main display area. The Access List Entries/New dialog box appears.
  - For Access List Number, enter **2**.
5. In the Access List Entries area, click the Add icon. The New Access List Entry dialog box appears. Configure the following, and then click **OK**:
  - For Sequence Number, enter **10**.
  - For Action, select **Permit**.
  - For Prefix, select **Prefix to Filter** and enter the IP address/netmask **1.1.1.1/24**.

6. Configure the route map:
  - In the virtual router navigation tree, select **Route Map**, and then click the Add icon in the main display area. The New Route Map dialog box appears.
  - For Name, enter **rtmap1**.
  - In the Route Map Entry area, click the Add icon. The New Route-Map Entry dialog box appears.
7. Configure the following way:
  - For Sequence Number, enter **10**.
  - For Action, select **permit**.
  - In the Match Properties area, in the access list table, select **2**.
  - Leave all other defaults and click **OK** to save the new route map entry.
8. Configure the export rule:
  - In the virtual router navigation tree, select **Export Rules**, and then click the Add icon in the main display area. The New Export Rule dialog box appears.
  - For Export to Virtual Router, select **untrust-vr**.
  - For Route Map, select **rtmap1**.
  - For Protocol, select **OSPF**.
9. Click **OK** to save the new export rule.
10. Click **OK** to save your changes to the virtual router, and then click **OK** again to save your changes to the device configuration.

In this example, you configure the trust-vr to automatically export all routes to the untrust-vr. You also configure a route map on the untrust-vr to permit only internal OSPF routes.

To configure trust-vr:

1. In the NSM navigation tree, select **Device Manager > Devices**. Double-click the device object to open the device configuration.
2. In Device Manager, double-click a device icon to open the device configuration. In the device navigation tree, select **Network > Virtual Routers**.
3. Configure the export rule for the trust-vr:
  - Double-click the trust-vr virtual router. The General Properties screen appears.
  - Select **Auto-export route to untrust-vr**.
  - Click **OK** to save your changes to the trust-vr.
4. Configure the route map for the untrust-vr.
  - Double-click the trust-vr virtual router. The General Properties screen appears.

- In the virtual router navigation tree, select **Route Map**, and then click the Add icon in the main display area.
  - For Name, enter **from-ospf-trust**.
5. In the Route Map Entry area, click the Add icon. The New Route-Map Entry dialog box appears.
    - For Sequence Number, enter **10**.
    - For Action, select **permit**.
    - In the Match Properties area, in the Route Type table, select **Internal OSPF**.
  6. Click **OK** to save the new route map entry, and then click **OK** again to save the route map.
  7. Click **OK** to save your changes to the virtual router, and then click **OK** again to save your changes to the device configuration.

**Related Documentation**

- [Configuring Virtual Routers on page 292](#)
- [Virtual Routers Overview on page 294](#)
- [Virtual Router General Properties Overview on page 295](#)
- [Access List Overview on page 296](#)
- [Route Map Overview on page 298](#)
- [Export and Import Rules in a Virtual Router Overview on page 300](#)
- [Example: Configuring Access Lists \(NSM Procedure\) on page 297](#)

## Routing Table Entries Overview

Typically, routers are attached to multiple networks and are responsible for directing traffic across these networks. Each router maintains a routing table, which is a list of known networks and directions on how to reach them. While processing an incoming packet on a security device, the router performs a routing table lookup to find the appropriate interface that leads to the destination address.

Each entry in a routing table—called a *route entry* or *route*—is identified by the destination network to which traffic can be forwarded. The destination network, in the form of an IP address and netmask, can be an IP network, subnetwork, supernet, or a host. Routing table entries can originate from the following sources:

- Directly connected networks (the destination network is the IP address that you assign to an interface in Route mode)
- Dynamic routing protocols, such as OSPF, BGP, or RIP
- Routes that are imported from other routers or virtual routers
- Statically configured routes

You can configure three types of static routes: destination-based, source-based, and source-interface-based routing. For each type of static route, you configure the following information:



**NOTE:** Source-interface-based routing is supported in ScreenOS 5.1 and later.

- The interface on the security device on which traffic for the destination network is forwarded.
- The next-hop, which can be either another virtual router on the security device or a gateway IP address (usually a router address).
- The protocol from which the route is derived.
- Preference (ScreenOS 5.1 and later only)—Controls the route to use when multiple routes to the same destination network exist. The lower the preference value of a route, the more likely the route is to be selected as the active route. By default, the preference value is automatically determined by the protocol or the origin of the route. You can modify a preference value from 1 to 255 for each protocol or route origin on a per-virtual router basis.
- Metric (ScreenOS 5.1 and later only)—Controls the route used when multiple routes for the same destination network with the same preference value exist. The metric value for connected routes is always 0. The default metric value for static routes is 1, but you can specify a different value from 1 to 255 when defining a static route.
- Keep route active when interface is down (ScreenOS 5.1 and later only)—Select this option to ensure that the route remains active even when the interface link status is down or the interface IP address is removed. By default, this option is disabled for all route entries. To enable this option for a destination-based route entry, you must configure the next-hop as a gateway (not a virtual router).
- The virtual system (vsys) to which this route belongs.



**NOTE:** In the routing table, you must configure a default route (network address 0.0.0.0/0) for the security device. You should also configure a route from the device to the IP address of the Network and Security Manager Device Server.

- Comment (ScreenOS 6.2 and later only)—Enables you to add a description to a static route that you configure. The description can be 1 to 32 characters in length. By specifying the description for a static route, you can identify the traffic that routes through the devices. It also allows you to search for a specific route in a route table when there are many static routes configured on the security device.

For instructions for configuring virtual router static route entries, see the *Network and Security Manager Online Help*.

- Related Documentation**
- [Route Types Overview on page 293](#)
  - [Virtual Routers Overview on page 294](#)
  - [Virtual Router General Properties Overview on page 295](#)
  - [Access List Overview on page 296](#)
  - [Route Map Overview on page 298](#)
  - [Destination-Based Routes Overview on page 305](#)

## Destination-Based Routes Overview

When a security device contains multiple virtual routers, the device does not automatically forward traffic between zones that reside in different VRs, even if the Security Policy permits that traffic. To enable traffic to pass from one virtual router to another, you can configure a static route in one virtual router that defines another VR as the next hop for the route. This route can even be the default route for the virtual router. For example, you can configure a default route for the trust-vr with the untrust-vr as the next hop. If the destination in an outbound packet does not match any other entries in the trust-vr routing table, it is forwarded to the untrust-vr.

To create a static route for a network destination, you must enter the IP address and netmask for the destination network, and then select either virtual router or gateway as the next hop:

- If the next hop is a virtual router, you must also select the VR that is to be the next hop for the route.
- If the next hop is a gateway, you must also enter the interface through which the next hop router is accessed, the IP address of the next hop router, and the metric and tag for the route.

For devices running ScreenOS 5.2, you can also configure gateway tracking to manage the route. When enabled, gateway tracking deactivates a route when the gateway becomes unreachable. When the gateway become reachable again, gateway tracking reactivates the route. Gateway tracking is supported only for destination-based route table entries. For devices running ScreenOS 6.3, destination-based routes supports IPv6.

For instructions for configuring virtual router destination-based route entries, see the *Network and Security Manager Online Help*.



**NOTE:** For security devices running ScreenOS 5.3, you can also configure source-based and source-interface-based routes with next hop as a virtual router within the same security device.

- Related Documentation**
- [Route Types Overview on page 293](#)
  - [Virtual Routers Overview on page 294](#)

- [Virtual Router General Properties Overview on page 295](#)
- [Access List Overview on page 296](#)
- [Route Map Overview on page 298](#)
- [Routing Table Entries Overview on page 303](#)
- [Source-Based Routes Overview on page 306](#)

---

## Source-Based Routes Overview

Some security devices also enable you to configure a route entry based on the source IP address of the data packet.

To create a static route for a network destination, you must enter the IP address and netmask for the destination network, then select the interface through which the next hop router is accessed. You must also enter the IP address of the next hop router and configure a metric for the route.

For instructions for configuring virtual router source-based route entries, see the *Network and Security Manager Online Help*.

### Related Documentation

- [Route Types Overview on page 293](#)
- [Virtual Routers Overview on page 294](#)
- [Virtual Router General Properties Overview on page 295](#)
- [Access List Overview on page 296](#)
- [Route Map Overview on page 298](#)
- [Routing Table Entries Overview on page 303](#)

---

## Example: Configuring Source-Based Routes (NSM Procedure)

In this example, you want to forward traffic from the 10.1.1.0/24 subnetwork to ISP 1, and forward traffic from the 10.1.2.0/24 subnetwork to ISP 2. You must configure two entries in the default trust-vr routing table and enable source-based routing. The subnetwork 10.1.1.0/24, with ethernet1 as the forwarding interface, uses the ISP 1 router (1.1.1.1) as the next hop; subnetwork 10.1.2.0/24, with ethernet2 as the forwarding interface, uses the ISP 2 router (2.2.2.2) as the next hop.

1. In the NSM navigation tree, select **Device Manager > Devices**. Double-click the device object to open the device configuration.
2. In the device navigation tree, select **Network > Virtual Routers**. Double-click the trust-vr virtual router. The General Properties screen appears.
3. In the virtual router navigation tree, select **Routing Table**.
4. Select **Enable Source-Based Routing**.

5. Add the first routing entry. In the Source-Based Routing Table area, click the Add icon. The New Source Routing Table dialog box appears.
6. Configure the following options:
  - For IP Address, enter **10.1.1.0**.
  - For Network Mask, enter **24**.
  - For Interface, select **ethernet1**.
  - For Gateway, enter the IP address **1.1.1.1**.
  - Click **OK** to save the new routing entry.
7. Add the second routing entry. In the Source-Based Routing Table area, click the Add icon. The New Source Routing Table dialog box appears.
8. Configure the following options:
  - For IP Address, enter **10.1.2.0**.
  - For Network Mask, enter **24**.
  - For Interface, select **ethernet2**.
  - For Gateway, enter the IP address **2.2.2.2**.
  - Click **OK** to save the new routing entry.
9. Click **OK** to save your changes to the device.

**Related  
Documentation**

- [Route Types Overview on page 293](#)
- [Virtual Routers Overview on page 294](#)
- [Virtual Router General Properties Overview on page 295](#)
- [Access List Overview on page 296](#)

## Source Interface-Based Routes Overview

Some security devices also enable you to configure a route entry based on the source interface (the interface on which a data packet arrives). You can use Source Interface-Based Routing (SIBR) to enable traffic from users on a specific subnet to be forwarded on one path while traffic from users on a different subnet is forwarded on another path.



**NOTE:** SIBR is supported in ScreenOS 5.1 and later.

SIBR can be used in conjunction with the source-based routing feature, which enables traffic to be forwarded based on the source IP address of a data packet. When a security device performs route lookup, the source interface-based routing table is checked first. If the route is not found in the source interface-based routing table and if source-based

routing is enabled, the source-based routing table is checked. If the route is not found in the source-based routing table, the destination-based routing table is checked.

You define source interface-based routes as static routes on a specific virtual router and source interface. Source interface-based routes only apply to the virtual router in which you configure them. For example, you cannot specify another virtual router as the next hop for a source interface-based route. You also cannot redistribute source interface-based routes into another virtual router or into a routing protocol.

When configuring SIBR, you must specify the name of the interface in the virtual router on which the packet arrives, and then set the interface on which the packet is to be forwarded. This interface can belong to a zone in another virtual router, if that virtual router is sharable. (Sharable virtual routers are VRs that are accessible by any vsys on the device. The untrust-vr is, by default, a sharable virtual router, but you can configure other root-level VRs to be sharable). Next, enter the IP address of the next-hop router in Gateway. If you have already specified a default gateway for the interface, you do not need to specify this parameter; the interface's default gateway is used for the source interface-based route.

You can also configure a metric for the route, if desired. By default, the metric for all SIBR entries is 1. If there are multiple source interface-based routes with the same prefix, only the route with the best (lowest) metric is used for route lookup and other routes with the same prefix are marked as "inactive."

For instructions for configuring virtual router source interface-based route entries, see the *Network and Security Manager Online Help*.

**Related  
Documentation**

- [Virtual Router General Properties Overview on page 295](#)
- [Access List Overview on page 296](#)
- [Route Map Overview on page 298](#)
- [Routing Table Entries Overview on page 303](#)
- [Destination-Based Routes Overview on page 305](#)
- [Source-Based Routes Overview on page 306](#)
- [Example: Source-Interface-Based Routing \(NSM Procedure\) on page 308](#)

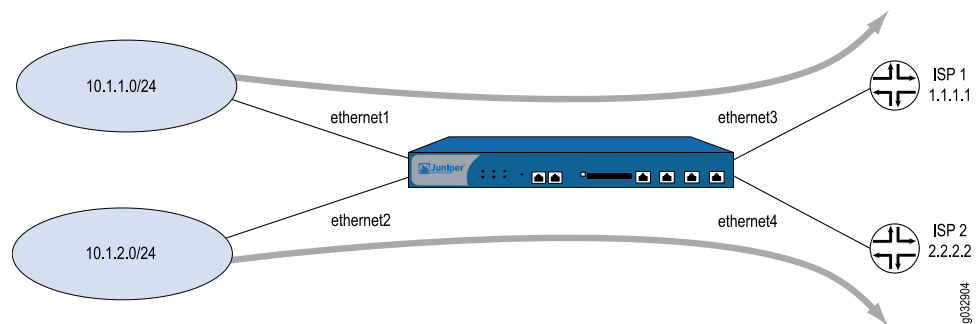
---

## Example: Source-Interface-Based Routing (NSM Procedure)

In this example, you want to forward traffic from the 10.1.1.0/24 subnetwork to ISP 1, and forward traffic from the 10.1.2.0/24 subnetwork to ISP 2. You must configure two entries in the default trust-vr routing table and enable source-based routing. The subnetwork 10.1.1.0/24, with ethernet2/1 as the source interface and ethernet2/3 as the forwarding interface, uses the ISP 1 router (1.1.1.1) as the next hop; subnetwork 10.1.2.0/24, with ethernet2/2 as the source interface and ethernet2/4 as the forwarding interface, uses the ISP 2 router (2.2.2.2) as the next hop.



Figure 5: Source Interface-Based Routing Overview



To configure source interface-based routing:

1. Add a NetScreen-5400 device running ScreenOS 5.x, and then configure the network module:
  - In the NSM navigation tree, select **Device Manager > Devices**. Double-click the device object to open the device configuration.
  - Double-click the device icon to open the device configuration. In the device navigation tree, select **Network > Slot**.
  - Double-click **slot 2** to display the slot configuration dialog box. For Card Type, select **5000-8G SPM**.
  - Click **OK** to save the slot configuration, and then click **Apply** to apply the new interfaces to the device.
2. Configure the ethernet 2/1 and ethernet 2/3 interfaces. In the device navigation tree, select **Network > Interface**.
3. Double-click the ethernet2/1 interface. The General Properties screen appears. Configure the following options:
  - For Zone, select **Trust**.
  - For IP address and Netmask, enter **10.1.1.0/24**.
  - Click **OK** to save your changes to the interface.
4. Double-click the ethernet2/3 interface. The General Properties screen appears. Configure the following options:
  - For Zone, select **Trust**.
  - For IP address and Netmask, enter **10.1.2.0/24**.
  - Click **OK** to save your changes to the interface.
5. In the device navigation tree, select **Network > Virtual Routers**. Double-click the trust-vr virtual router. The General Properties screen appears. In the router navigation tree, select **Routing Table**.
6. Select **Enable Source-Based Routing**.

7. Configure the first entry. In the Source Interface-Based Routing Table area, click the Add icon.
8. Configure the following options:
  - For Incoming Interface, select **ethernet2/1**.
  - For IP Address and Netmask, enter **10.1.1.0/24**
  - For Interface, enter **ethernet2/3**.
  - For Gateway IP Address, enter **1.1.1.1**
  - Click **OK** to save the SIBR entry.
9. Configure the second entry. In the Source Interface-Based Routing Table area, click the Add icon.
10. Configure the following:
  - For Incoming Interface, select **ethernet2/3**.
  - For IP Address and Netmask, enter **10.1.2.0/24**
  - For Interface, enter **ethernet2/4**.
  - For Gateway IP Address, enter **2.2.2.2**
  - Click **OK** to save the SIBR entry.
11. Click **OK** to save your changes to the virtual router, and then click **OK** to save your changes to the device.

- Related Documentation**
- [Destination-Based Routes Overview on page 305](#)
  - [Source-Based Routes Overview on page 306](#)

---

## Configuring Route Preferences

---

A route preference is a weight added to the route that influences the determination of the best path for traffic to reach its destination. When importing or adding a route to the routing table, the virtual router adds a preference value—determined by the protocol by which the route is learned—to the route. A low preference value (a number closer to 0) is preferable to a high preference value (a number further from 0). In a virtual router, you can set the preference value for routes according to protocol.

To change the preference value for a protocol, enter a new value for the protocol in the Route Preferences configuration screen.

- Related Documentation**
- [Route Types Overview on page 293](#)
  - [Access List Overview on page 296](#)
  - [Route Map Overview on page 298](#)
  - [Routing Table Entries Overview on page 303](#)
  - [Destination-Based Routes Overview on page 305](#)

- [Source Interface-Based Routes Overview on page 307](#)
- [Dynamic Routing Configuration Overview on page 311](#)

---

## Dynamic Routing Configuration Overview

---

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

- [“OSPF Protocol Configuration Overview” on page 311](#)
- [RIP Overview on page 319](#)
- [BGP Overview on page 325](#)

### Related Documentation

- [Source Interface-Based Routes Overview on page 307](#)
- [Configuring Route Preferences on page 310](#)

---

## OSPF Protocol Configuration Overview

---

The OSPF routing protocol operates within a single autonomous system (AS). A router running OSPF distributes its state information (such as usable interfaces and neighbor reachability) by periodically flooding link-state advertisements (LSAs) throughout the AS.

Each OSPF router uses LSAs from neighboring routers to maintain a linkstate database, a listing of topology and state information for the surrounding networks. The constant distribution of LSAs throughout the routing domain enables all routers in an AS to maintain identical link-state databases. OSPF uses the link-state database to determine the best path to any network within the AS by generating a shortest-path tree (a graphical representation of the shortest path to any network within the AS). While all routers have the same link-state database, they all have unique shortest-path trees because a router always generates the tree with itself at the top of the tree.

To enable OSPF on a security device, you must first enable OSPF on a virtual router, and then enable OSPF on individual interfaces. You can also configure optional OSPF settings, such as the following:

- Global settings, such as virtual links, that are set at the VR level for the OSPF protocol.
- Interface settings, such as authentication, that are set on a per-interface basis for the OSPF protocol. When you configure an OSPF parameter at the interface level, the parameter setting affects the OSPF operation only on the specific interface.

Additionally, you can set security-related OSPF settings at either the VR level or on a per-interface basis. The following topics detail how to enable OSPF and configure all optional parameters.

### Related Documentation

- [Route Types Overview on page 293](#)
- [Route Map Overview on page 298](#)

- [Routing Table Entries Overview on page 303](#)
- [Configuring Route Preferences on page 310](#)
- [Dynamic Routing Configuration Overview on page 311](#)
- [Global OSPF Settings Overview on page 313](#)
- [Configuring OSPF Interface Parameters Overview on page 315](#)

---

## Enabling OSPF (NSM Procedure)

---

To enable OSPF on a security device, you must first create an OSPF instance on a virtual router, and then enable OSPF on individual interfaces.

To create an OSPF instance in a virtual router:

1. In the NSM navigation tree, select **Device Manager > Devices**. Double-click the device object to open the device configuration.
2. In the device navigation tree, select **Network > Virtual Router** and double-click the virtual router for which you want to configure OSPF.
3. In the virtual router navigation tree, select **Dynamic Routing Protocol**, and then select **Configured OSPF Instance**. The OSPF settings appear in the router navigation tree.
4. Select **OSPF > Parameters**, and then select **Enable OSPF**. If desired, configure additional global and security settings, as detailed in [“Global OSPF Settings Overview” on page 313](#).
5. Click **OK** to save your changes to the virtual router.

To enable OSPF on an interface:

1. In the NSM navigation tree, select **Device Manager > Devices**. Double-click the device object to open the device configuration.
2. In the device navigation tree, select **Network > Interface** and double-click the interface for which you want to configure OSPF.
3. In the interface navigation tree, select **Protocol** and select the **OSPF** tab.
4. Select **Enable OSPF**. If desired, configure additional interface and security settings, as detailed in [“Configuring OSPF Interface Parameters Overview” on page 315](#).
5. Click **OK** to save your changes to the interface.

### Related Documentation

- [Configuring Route Preferences on page 310](#)
- [Dynamic Routing Configuration Overview on page 311](#)
- [OSPF Protocol Configuration Overview on page 311](#)
- [Global OSPF Settings Overview on page 313](#)
- [Configuring OSPF Interface Parameters Overview on page 315](#)

- [Configuring OSPF \(NSM Procedure\) on page 318](#)

## Global OSPF Settings Overview

A global OSPF setting affects operations on all OSPF-enabled interfaces. You configure global settings in the virtual router.

For instructions on configuring OSPF settings on the virtual router and on the interface, see the *Network and Security Manager Online Help*.

## Configuring OSPF Parameters

The OSPF instance parameters are displayed in [Table 77 on page 313](#).

**Table 77: OSPF Instance Parameters**

Parameters	Your Action
Automatically Generate Virtual Links	Select this option to direct the VR to automatically create a virtual link for instances when it cannot reach the network backbone. By default, this option is disabled.
Reject Default Route	Select this option to prevent Route Detour Attacks, in which a router injects a default route (0.0.0.0/0) into the routing domain to detour packets to itself. During a router detour, a compromised router can then either drop the packets, causing service disruption, or it can obtain sensitive information in the packets before forwarding them. By default, this option is disabled, meaning OSPF accepts any default routes that are learned in OSPF and adds the default route to the routing table.
RFC 1583 Compatible	Select this option to make the OSPF routing instance compatible with RFC 1583, an earlier version of OSPF. By default, security devices support OSPF version 2, as defined by RFC 2328.
Prevent Hello Packet Flooding Attack	Configure the Maximum Hello Packets threshold accepted by the VR. By default, the OSPF hello packet threshold is 10 packets per hello interval. You might want to use this setting to prevent a malfunctioning or compromised router from flooding its neighbors with OSPF hello packets.
Prevent LSA Flooding Attack	Configure the number of LSAs accepted by the VR. By default, the VR accepts all LSAs. You might want to use this setting to prevent a malfunctioning or compromised router from flooding its neighbors with OSPF LSA packets. During an LSA flood attack, a router generates an excessive number of LSAs in a short period of time, thus keeping other OSPF routers in the network busy running the SPF algorithm.
Advertising Default Route	Select this option to direct the VR to advertise an active default route (0.0.0.0/0) in the VR route table to all OSPF areas.

## Configuring OSPF Areas

By default, all routers are grouped into a single “backbone” area called area 0 (usually denoted as area 0.0.0.0). However, you might want to segment large geographically dispersed networks into multiple areas for better scalability.

Using multiple areas reduces the amount of routing information passed throughout the network because a router only maintains a link-state database for the area in which it resides. The VR maintains link-state information for all connected areas, and does not maintain link-state information for networks or routers outside the area.

AS external advertisements describe routes to destinations in other autonomous systems and are flooded throughout an AS. To prevent AS external advertisements from flooding an AS, configure the OSPF area as a stub area:

- Stub area—An area that receives route summaries from the backbone area but does not receive link-state advertisements from other areas for routes learned through non-OSPF sources (BGP, for example). A stub area can be considered a totally stubby area if no summary routes are allowed in the stub area.
- Not So Stubby Area (NSSA)—Like a normal stub area, NSSAs cannot receive routes from non-OSPF sources outside the current area. However, external routes learned within the area can be learned and passed to other areas.

All areas must connect to area 0, which is defined by default on the virtual router when you enable the OSPF routing instance on the virtual router. For areas that cannot be physically connected to the backbone area, you must configure a virtual link to provide the remote area with a logical path to the backbone through another area. For details on virtual links, see [“Configuring OSPF Virtual Links” on page 315](#).

## Configuring OSPF Summary Import

In large internetworks where hundreds or even thousands of network addresses can exist, routers can become overly congested with route information. After you have redistributed a series of routes from an external protocol to the current OSPF routing instance, you can bundle the routes into one generalized or summarized network route. By summarizing multiple addresses, you enable a series of routes to be recognized as one route, simplifying the process.

Using route summarization in a large, complex network can isolate topology changes from other routers. An intermittently failing link in a domain does not affect the summary route, so no router external to the domain needs to modify its routing table due to the link failure. Route summarization also prevents LSAs from propagating to other areas when a summarized network goes down or comes up.

You can summarize inter area routes or external routes.

## Configuring OSPF Redistribution Rules

Use route redistribution to exchange route information between routing protocols. You can redistribute the following types of routes into the OSPF routing instance in the same VR:

- Routes learned from BGP
- Directly connected routes
- Imported routes
- Statically configured routes

When you configure route redistribution, you must first specify a route map to filter the routes that are redistributed.

## Configuring OSPF Virtual Links

All areas must connect to area 0, which is the backbone. Area 0 is defined by default on the virtual router when you enable the OSPF routing instance on the virtual router. For areas that cannot be physically connected to the backbone area, you must configure a virtual link to provides the remote area with a logical path to the backbone through another area.

To enable a virtual link, the virtual link must exist on routers at both ends of the link. Specifically, you must configure:

- Area ID—The ID of the OSPF area through which the virtual link passes. You cannot create a virtual link that passes through the backbone area or a stub area.
- Router ID—The ID of the router at the other end of the virtual link.

### Related Documentation

- [Configuring Route Preferences on page 310](#)
- [Dynamic Routing Configuration Overview on page 311](#)
- [OSPF Protocol Configuration Overview on page 311](#)
- [Configuring OSPF Interface Parameters Overview on page 315](#)

## Configuring OSPF Interface Parameters Overview

By default, OSPF is disabled on all interfaces in the VR. You must enable OSPF on an interface before OSPF can use that interface to transmit receive packets. When you disable OSPF on an interface, OSPF does not transmit or receive packets on the specified interface, but interface configuration parameters are preserved.

For instructions for configuring OSPF settings on the virtual router and on the interface, see the *Network and Security Manager Online Help*.

You can enable OSPF on Ethernet and tunnel interfaces. When configuring OSPF on a tunnel interface, you can configure additional parameters to keep OSPF tunnel traffic to a minimum.

The OSPF interface parameters are displayed in [Table 78 on page 316](#).

Table 78: OSPF Interface Parameters

Parameters	Your Action
Bind to Area	Select a previously created area to bind the interface to that area. By default, all interfaces are bound to area 0, the backbone area.
Cost	Configure the metric for the interface. The cost associated with an interface depends upon the bandwidth of the link to which the interface is connected. The higher the bandwidth, the lower (more desirable) the cost value.
Hello Interval	Configure the number of seconds that the interface sends out OSPF hello packets to the network. By default, the interface sends 10 hello packets per second.
OSPF Priority	Configure the priority level of the VR elected by the interface. The router (designated router or backup designated router) with the larger priority value has the best chance (although not guaranteed) of being elected.
Retransmit Interval	Configure the number of seconds that elapse before the interface resends an LSA to a neighbor that did not respond to the original LSA. By default, the interface resends an unacknowledged LSA every 5 seconds.
Transmit Delay	Configure the number of seconds between transmissions of link-state update packets sent on the interface. By default, the interface sends link-state updates every second.
Configuring Interface Link Type	Configure how the interface forms adjacencies with other routers: <ul style="list-style-type: none"> <li>• A point-to-point interface for OSPF forms an adjacency with only one OSPF router in the area. If the local tunnel interface is to be bound to multiple tunnels, you must configure the local tunnel interface as a point-to-multipoint interface.</li> <li>• A regular multicast interface for OSPF acts as a broadcast interface, and forms adjacencies with all routers in the area.</li> </ul>
Enable Reduction in LSA Flooding (ScreenOS 5.1 and later only)	Select to suppress LSA packets. When this option is enabled, the device sends LSA packets only when the LSA content has changed. By default, this option is disabled.
Configure to Ignore MTU Mismatch in DB Exchange (ScreenOS 5.1 and later only)	Select to ignore any mismatches in maximum transmission unit (MTU) values between the local and remote interfaces that are found during OSPF database negotiations. Use this option only when the MTU on the local interface is lower than the MTU on the remote interface.
Interface OSPF Passive Mode	Select to prevent the interface from transmitting or receiving packets. The IP address of the interface is still advertised on the OSPF domain as an OSPF route and not as an external route. You might want to select this option when BGP is also enabled on the interface.

In addition you can configure OSPF demand circuit for ScreenOS 5.1 and later tunnel interfaces only. An OSPF demand circuit is a network segment on which connect time



or usage affects the cost of using such a connection. When traversing a demand circuit, the security device limits routing protocol traffic to changes in network topology, and suppresses sending OSPF hello packets and periodic refreshment of LSA flooding.

- To configure an interface as a demand circuit:
  - The interface link type must be point-to-point or serial; you cannot configure a point-to-multipoint interface as a demand circuit.
  - You must configure both ends of the tunnel as demand circuits.

## Configuring OSPF Neighbors

Two routers with interfaces on the same subnet are considered neighbors. Routers use the hello protocol to establish and maintain these neighbor relationships. When two routers establish bidirectional communication, they are said to have established an adjacency. If two routers do not establish an adjacency, they cannot exchange routing information. By default, the OSPF routing instance on the virtual router forms adjacencies with all OSPF neighbors communicating on an OSPF-enabled interface.

You can configure the following settings for neighbors on the interface:

- Neighbor Dead Interface—Enter the number of seconds that elapses with no response from an OSPF neighbor before OSPF determines the neighbor is not running. By default, OSPF determines a neighbor is “dead” after 40 seconds.
- Add/Edit/Delete Neighbor (Ethernet Interface Only)—To limit the devices on an interface that can form adjacencies with the OSPF routing instance, define the subnets that contain eligible OSPF neighbors. Only hosts or routers that reside in the specified subnets can form adjacencies with the OSPF routing instance.



**NOTE:** All OSPF routers in an area must use the same hello, dead, and retransmit interval values before they can form adjacencies.

## Configuring OSPF Authentication

Because LSAs are unencrypted, most protocol analyzers can decapsulate OSPF packets. Authenticating OSPF neighbors using MD5 authentication or simple password is the best way to fend off these types of attacks.

When authentication is enabled, the device discards all unauthenticated OSPF packets received on the interface. By default, authentication is disabled.

To enable authentication, select one of the following authentication methods:

- Clear Text Authentication—To use a simple password for authentication, select this option and enter the password.



**NOTE:** All passwords handled by NSM are case-sensitive.

- Multiple MD5 Authentication— To use MD5 keys for authentication, select this option, and then configure the active MD5 key.
  - To use an existing MD5 key, select the key ID as the active MD5 key ID.
  - To add a new MD5 key, click the Add icon and configure a key ID for the new MD5 key.



**NOTE:** You must use the same MD5 key for the sending and receiving OSPF routers.

**Related  
Documentation**

- [Configuring Route Preferences on page 310](#)
- [Dynamic Routing Configuration Overview on page 311](#)
- [OSPF Protocol Configuration Overview on page 311](#)
- [Global OSPF Settings Overview on page 313](#)

---

## Configuring OSPF (NSM Procedure)

---

To configure OSPF:

1. In the NSM navigation tree, select **Device Manager > Devices**. Double-click the device object to open the device configuration.
2. In the device navigation tree, select **Network > Virtual Router** to display the list of configured virtual routers. Double-click the virtual router in which you are configuring an OSPF routing instance. The Virtual Router configuration screen appears.
3. In the virtual router navigation tree, select **Dynamic Routing Protocol** and enable **Configured OSPF Instance** check box. OSPF configuration options now appear in the virtual router navigation tree under Dynamic Routing Protocol.
4. In the virtual router navigation tree, select **OSPF > Parameters** to display the Parameters screen. Select **OSPF**, and then click **OK** to close the Parameters screen.
5. To define a new non-backbone OSPF area:
  1. Select **OSPF > Area**. The Area configuration screen appears. In this screen, do the following:
    - Click the Add icon.
    - Enter ID in the Area ID box.
    - Select the interfaces that are to be included in this OSPF area.
    - Select the Type.
  2. Click **OK** to close the Area configuration screen.

6. In the device navigation tree, select **Network > Interface** to display the list of interfaces. Double-click the interface that is connected to OSPF peers to open the interface screen.
7. In the interface navigation tree, select **Protocol** to display the Protocol screen, then click the **OSPF** tab and configure the following:
8. Select the ID of the OSPF area to which the interface is bound.
9. Select **OSPF**.
10. Click **OK**.

#### Related Documentation

- [Configuring Route Preferences on page 310](#)
- [Dynamic Routing Configuration Overview on page 311](#)
- [OSPF Protocol Configuration Overview on page 311](#)
- [Global OSPF Settings Overview on page 313](#)
- [Configuring OSPF Interface Parameters Overview on page 315](#)
- [RIP Overview on page 319](#)
- [Enabling OSPF \(NSM Procedure\) on page 312](#)

## RIP Overview

Routing Information Protocol (RIP) is a distance vector protocol used in moderate-sized autonomous systems (AS). Security devices support RIPv1 and RIPv2 (as defined by RFC 2453) and additional MD5 authentication extensions (as defined by RFC 2082).

Use RIP for dynamic routing on moderate-sized networks and to manage route information within a small, homogeneous, network such as a corporate LAN. The longest path allowed in a RIP network is 15 hops; a metric value of 16 indicates an invalid or unreachable destination. RIP supports both point-to-point networks (used with VPNs) and broadcast or multicast Ethernet networks. RIP does not support point-to-multipoint interfaces.

RIP maintains its own database of routes, including RIP protocol routes and redistributed routes. This database contains one entry for every destination that is reachable through the RIP routing instance. RIP adds the best routes to the VR routing table based on the virtual router's ECMP limit (configured in the General Properties area of the virtual router) and the alternate route limit (configured in the virtual router's RIP parameters). RIP sends out messages that contain the complete routing table to every neighboring router every 30 seconds. These messages are normally sent as multicasts to address 224.0.0.9 from the RIP port.

To enable RIP on a security device, you must first enable RIP on a virtual router, then enable RIP on individual interfaces. You can also configure optional RIP settings, such as the following:

- Global settings, such as timers and trusted RIP neighbors, that are set at the VR level for the RIP protocol.

- Interface settings, such as authentication, that are set on a per-interface basis for the RIP protocol. When you configure a RIP parameter at the interface level, the parameter setting affects the RIP operation only on the specific interface.

Additionally, you can set security-related RIP settings at either the VR level or on a per-interface basis.

**Related  
Documentation**

- [Route Types Overview on page 293](#)
- [Virtual Router General Properties Overview on page 295](#)
- [OSPF Protocol Configuration Overview on page 311](#)
- [Global RIP Settings Overview on page 321](#)
- [RIP Interface Parameters Overview on page 323](#)
- [BGP Overview on page 325](#)

---

## Configuring RIP (NSM Procedure)

---

To enable RIP on a security device, you must first create a RIP instance on a virtual router, and then enable RIP on individual interfaces.

To create a RIP instance on a virtual router:

1. In the NSM navigation tree, select **Device Manager > Devices**. Double-click the device object to open the device configuration.
2. In the device navigation tree, select **Network > Virtual Router** and double-click the virtual router for which you want to configure RIP.
3. In the virtual router navigation tree, select **Dynamic Routing Protocol** and enable **Configured RIP Instance** check box. The RIP settings appear in the router navigation tree.
4. Select **RIP > Parameters**, and then select **Enable RIP** check box. If desired, configure additional global and security settings, as detailed in [“Global RIP Settings Overview” on page 321](#).
5. Click **OK** to save your changes to the virtual router.

To enable RIP on an interface:

1. In the device navigation tree, select **Network > Interface** and double-click the interface for which you want to configure RIP.
2. In the interface navigation tree, select **Protocol** and select the **RIP** tab.
3. Select **Enable RIP**. If desired, configure additional interface and security settings, as detailed in [“RIP Interface Parameters Overview” on page 323](#).
4. Click **OK** to save your changes to the interface.

**Related  
Documentation**

- [Configuring Route Preferences on page 310](#)

- [Dynamic Routing Configuration Overview on page 311](#)
- [OSPF Protocol Configuration Overview on page 311](#)
- [RIP Overview on page 319](#)
- [Global RIP Settings Overview on page 321](#)
- [RIP Interface Parameters Overview on page 323](#)

## Global RIP Settings Overview

A global RIP setting affects operations on all RIP-enabled interfaces. You configure global settings in the virtual router.

For instructions for configuring RIP settings on the virtual router and on the interface, see the *Network and Security Manager Online Help*.

## Configuring RIP Parameters

You can configure the RIP instance parameters displayed in [Table 79 on page 321](#).

**Table 79: RIP Instance Parameters**

Parameters	Your Action
RIP Version (ScreenOS 5.1 and later only)	Select the version of RIP you want to use for this virtual router. When you configure RIP on the individual interfaces, you can override this setting.
Reject Default Route	Select this option to prevent route detour attacks in which a router injects a default route (0.0.0.0/0) into the routing domain to detour packets to itself. During a route detour attack, a compromised router can drop the packets, causing service disruption, or can obtain sensitive information in the packets before forwarding them. By default, this option is disabled, meaning RIP accepts any default routes that are learned in RIP and adds the default route to the routing table.
Ignore Same Subnet Checking	Select this option to allow RIP neighbors on different subnets.
Advertising Default Route	Select this option to direct the VR to advertise an active default route (0.0.0.0/0) in the VR route table to all RIP areas.
Default Metric	Configure the default metric for routes that RIP imports from other protocols, such as OSPF and BGP. By default, RIP assigns a metric of 10 to all imported routes.
Number of Alternate Routes for Prefix Allowed (ScreenOS 5.1 and later only)	Configure the maximum number of RIP routes for the same prefix that RIP can add to the RIP route database. By default, RIP does not allow alternate routes.

Table 79: RIP Instance Parameters (*continued*)

Parameters	Your Action
Hold Down Time for Routes (ScreenOS 5.1 and later only)	<p>Configure the number of seconds that RIP waits before updating the routing table. Use this option to prevent route flapping when handling high metric routes. By default, RIP waits 120 seconds between routing table updates. When configuring this option:</p> <ul style="list-style-type: none"> <li>• Ensure that the value is at least three times the value of the Update Timer.</li> <li>• Ensure that the value does not exceed the sum of the Update Timer value plus the Flush Timer value.</li> </ul> <p>For example, if the Update Timer is 60 and the Flush Timer is 180, you can set the hold down time value between 181 and 239.</p>
Retransmit Interval for Demand Circuits (ScreenOS 5.1 and later only)	<p>Configure the number of seconds that elapse before RIP resends the RIP routing table to a demand circuit neighbor that did not respond. You can also configure the number of times RIP attempts to retransmit the routing table. By default, RIP resends every 5 seconds.</p>
Poll Interval for Demand Circuits (ScreenOS 5.1 and later only)	<p>Configure the number of seconds between demand circuit checks. By default, RIP sends a request through the demand circuit every three minutes to verify that the tunnel interface is up. You can also configure the number of times a demand circuit must fail to respond before RIP considers the circuit down. By default, RIP never considers an unresponsive circuit down (Number of Retries is 0).</p>
Timers	<p>Configure the following timers:</p> <ul style="list-style-type: none"> <li>• Update Timer—Configure the number of seconds that the virtual router sends RIP route database updates to neighbors.</li> <li>• Invalid Timer—Configure the number of seconds after a neighbor stops advertising a route that RIP considers the route invalid. By default, RIP considers a route invalid 180 seconds after a neighbor stops advertising it.</li> <li>• Flush Timer—Configure the number of seconds an invalid route remains in the RIP route database. By default, RIP removes a route that has been invalid for 120 seconds.</li> </ul>
Maximum Route Update Packets	<p>Configure the maximum number of packets that the VR can receive per RIP update.</p>
Maximum Neighbors Allowed on One Interface	<p>Configure the maximum number of RIP neighbors allowed on a single interface. By default, RIP allows up to 16 neighbors for the same interface.</p>
Access List for Filtering Trusted Neighbors	<p>Configure the access list that defines trusted RIP neighbors. If you do not select an access list, RIP uses multicasting or broadcasting to detect neighbors on a RIP-enabled interface.</p>
Route Maps	<p>To control which routes RIP learns and advertises, configure the following:</p> <ul style="list-style-type: none"> <li>• The inbound route map defines the routes that RIP learns.</li> <li>• The outbound route map defined the routes that RIP advertises.</li> </ul>

## Configuring RIP Redistribution Rules

Use route redistribution to exchange route information between routing protocols. You can redistribute the following types of routes into the RIP routing instance in the same VR:

- Routes learned from BGP
- Routes learned from OSPF
- Directly connected routes
- Imported routes
- Statically configured routes

When you configure route redistribution, you must first specify a route map to filter the routes that are redistributed.

## Configuring RIP Summary Import (ScreenOS 5.1 and later only)

In large internetworks where hundreds or even thousands of network addresses can exist, routers can become overly congested with route information. After you have redistributed a series of routes from an external protocol to the current RIP routing instance, you can bundle the routes into one generalized or summarized network route. By summarizing multiple addresses, you enable a series of routes to be recognized as one route, simplifying the process.

Using route summarization in a large, complex network can isolate topology changes from other routers. An intermittently failing link in a domain does not affect the summary route, so no router external to the domain needs to modify its routing table due to the link failure.

You can summarize inter area routes or external routes.

### Related Documentation

- [Configuring Route Preferences on page 310](#)
- [Dynamic Routing Configuration Overview on page 311](#)
- [OSPF Protocol Configuration Overview on page 311](#)
- [RIP Overview on page 319](#)
- [RIP Interface Parameters Overview on page 323](#)

## RIP Interface Parameters Overview

By default, RIP is disabled on all interfaces in the VR. You must enable RIP on an interface before RIP can use that interface to transmit receive packets. When you disable RIP on an interface, RIP does not transmit or receive packets on the specified interface, but interface configuration parameters are preserved.

For instructions for configuring RIP settings on the virtual router and on the interface, see the *Network and Security Manager Online Help*.

You can enable RIP on ethernet and tunnel interfaces. When configuring RIP on a tunnel interface, you can configure additional parameters to keep RIP tunnel traffic to a minimum.

You can configure the following RIP interface parameters:

- **Bind Interface to RIP**—Select to bind this interface to RIP.
- **Run Demand Circuit** (ScreenOS 5.1 and later tunnel interface only)—Configure the tunnel interface as a RIP demand circuit (a network segment on which connect time or usage affects the cost of using such connection). When traversing a demand circuit, the security device limits routing protocol traffic to changes in network topology, and suppresses sending RIP packets. To complete the demand circuit, you must configure both ends of the tunnel as demand circuits.
- **Enable Summarization** (ScreenOS 5.1 and later only)—Select to enable route summarization on this interface. By default, the interface does not allow route summarization.
- **Add/Edit/Delete RIP Neighbor** (ScreenOS 5.1 and later only)—You can define the static RIP neighbors for the interface.
- **RIP Versions** (ScreenOS 5.1 and later only)—Select the version of RIP you want this interface to use for sending and receiving RIP information. By default, the interface uses the RIP version configured for the virtual router (Vrouter RIP Instance Version); if you select a different version, it overrides the virtual router setting.
- **Metric**—Configure the metric used for RIP routes from this interface.
- **Passive Mode**—Select to prevent the interface from transmitting packets (the interface can still receive packets). RIP advertises the IP address of the interface as a RIP route and not as an external route. By default, passive mode is disabled; however, you might want to select this option when BGP is also enabled on the interface.
- **Route Maps**—To control which routes RIP learns and advertises, select a previously created route map for each of the following:
  - The Incoming Route Map Filter defines the routes that RIP learns.
  - The Outgoing Route Map Filter defines the routes that RIP advertises.These settings override the route maps configured on the virtual router.
- **Split Horizon**—Select **Split-Horizon** to prevent the interface from advertising learned routes in RIP updates sent to the same interface. When enabled, you can also select the **Poison Reverse** option, which instructs the interface to advertise learned routes with a metric of 16 when sending updates to the same interface. By default, split horizon is disabled.

## Configuring RIP Authentication

Because RIP packets are unencrypted, most protocol analyzers can decapsulate them. Authenticating RIP neighbors using MD5 authentication or simple password is the best way to fend off these types of attacks. When authentication is enabled, the device discards all unauthenticated RIP packets received on the interface. By default, authentication is disabled.



To enable authentication, select one of the following authentication methods:

- Clear Text Authentication—To use a simple password for authentication, select this option and enter the password.



**NOTE:** All passwords handled by NSM are case-sensitive.

- Multiple MD5 Authentication— To use MD5 keys for authentication, select this option, and then configure the active MD5 key.
  - To use an existing MD5 key, select the key ID as the Active MD5 Key ID.
  - To add a new MD5 key, click the Add icon and configure a Key ID for the new MD5 key.



**NOTE:** You must use the same MD5 key for the sending and receiving RIP routers.

#### Related Documentation

- [RIP Overview on page 319](#)
- [Global RIP Settings Overview on page 321](#)
- [BGP Overview on page 325](#)

## BGP Overview

Border Gateway Protocol (BGP) is a path-vector protocol that is used to carry routing information between autonomous systems (ASs). To configure BGP, you must create and enable the BGP routing instance in a virtual router by assigning an autonomous system number to the BGP instance, and then enabling the instance. After you enable and configure the BGP peer, you can then enable BGP on the interface that is connected to the peer.

Before two BGP devices can communicate and exchange routes, they need to identify each other so they can start a BGP session. You need to specify the IP addresses of the BGP peers and, optionally, configure parameters for establishing and maintaining the session. Peers can be either internal (IBGP) or external (EBGP) peers. For an EBGP peer, you need to specify the autonomous system in which the peer resides.

All BGP sessions are authenticated by checking the BGP peer identifier and the AS number advertised by the peers. A successful connection with a peer is logged. If anything goes wrong with the peer connection, a BGP notification message is sent to or received from the peer, which causes the connection to fail or close.

For instructions for configuring BGP settings on the virtual router and on the interface, see the *Network and Security Manager Online Help*.

**Related Documentation**

- [Source Interface-Based Routes Overview on page 307](#)
- [Configuring Route Preferences on page 310](#)
- [Dynamic Routing Configuration Overview on page 311](#)
- [OSPF Protocol Configuration Overview on page 311](#)
- [RIP Overview on page 319](#)
- [Route-Refresh Capabilities Overview on page 326](#)
- [Configuring BGP Networks on page 327](#)

---

## Route-Refresh Capabilities Overview

---

NSM supports BGP route-refresh. This feature provides a soft reset mechanism that allows the dynamic exchange of route refresh requests and routing information between BGP peers and the subsequent re-advertisement of the outbound or inbound routing table.

Routing policies for a BGP peer using route-maps might impact inbound or outbound routing table updates because whenever a route policy change occurs, the new policy takes effect only after the BGP session is reset. A BGP session can be cleared through a hard or soft reset.



**NOTE:** A hard reset is disruptive because active BGP sessions are torn down and brought back up.

A soft reset allows the application of a new or changed policy without clearing an active BGP session. The route-refresh feature allows a soft reset to occur on a per-neighbor basis and does not require preconfiguration or extra memory.

A dynamic inbound soft reset generates inbound updates from a neighbor. An outbound soft reset sends a new set of updates to a neighbor. Outbound resets do not require preconfiguration or routing table update storage.

The route-refresh feature requires that both BGP peers advertise route-refresh feature support in the OPEN message. If the route-refresh method is successfully negotiated, either BGP peer can use the route-refresh feature to request full routing information from the other end.

For more detailed information about zones on security devices, see the *Concepts & Examples ScreenOS Reference Guide: Routing*.

**Related Documentation**

- [RIP Overview on page 319](#)
- [Global RIP Settings Overview on page 321](#)
- [RIP Interface Parameters Overview on page 323](#)
- [Route-Refresh Capabilities Overview on page 326](#)

- [BGP Overview on page 325](#)
- [Configuring BGP Networks on page 327](#)

## Configuring BGP Networks

Use the BGP network settings to change the route attributes generated by BGP. For each route you want to change, create a new network entry that contains the IP address and netmask for the network reachable from the BGP routing instance. Next, configure the new route attributes for that network. On devices running ScreenOS 6.3, BGP network supports IPv6. The BGP network settings are displayed in [Table 80 on page 327](#).

**Table 80: BGP Network Settings**

Parameters	Your Action
Check Route Availability	<p>Configure how BGP determines route availability for this route:</p> <ul style="list-style-type: none"> <li>• Turn Off Reachability Check—When enabled, the BGP routing instance does not test whether it can reach the specified network.</li> <li>• Check for Same Route—When enabled, the BGP routing instance checks the prefix entered after the network for reachability; if reachable, the BGP routing instance adds the network.</li> <li>• Check Route Reachability—Select to direct the BGP routing instance to perform a test to determine whether it can reach the network you identified.</li> </ul>
Configure Route Attributes (ScreenOS 5.1 and later only)	<p>Configure how BGP determines the route attributes for the specified route:</p> <ul style="list-style-type: none"> <li>• Weight—Select <b>Weight</b> to assign a local preference value to the route that is not advertised to peers. If BGP uses more than one route to a destination, the route with the highest weight value is preferred.</li> <li>• Route Map—Select a previously-created route map to apply attributes for this route. BGP advertises the route with the route attributes specified in the selected route map.</li> </ul>

### Related Documentation

- [BGP Overview on page 325](#)
- [Route-Refresh Capabilities Overview on page 326](#)
- [Configuring Aggregate Addresses on page 327](#)
- [Configuring Neighbors and Peer Groups Overview on page 328](#)
- [Configuring a BGP Routing Instance \(NSM Procedure\) on page 329](#)

## Configuring Aggregate Addresses

As the number of BGP router addresses grows, each route in the AS requires more memory and CPU time to process addresses from the routing table. Using aggregation, BGP can reduce the size of a routing table by summarizing a range of addresses into a single route entry. Each address range included in the aggregate address is considered a contributing route within the aggregate address.

For each aggregate address you want to use, create an aggregate address entry that contains the aggregate address IP and netmask. Next, configure the route attributes for the address. The aggregate address configuration details are displayed in

[Table 81 on page 328](#).

**Table 81: Aggregate Address**

Parameters	Your Action
AS Set	When enabled, BGP generates AS set-path information for the aggregated route and all contributing routes.
Summary Only	When enabled, BGP advertises the aggregate route in place of individual addresses for more specific contributing routes. If you select this option, you cannot configure a Suppress Route Map entry for this aggregate route.
Route Maps (ScreenOS 5.1 and later only)	<p>Configure a previously created route map for each of the following:</p> <ul style="list-style-type: none"> <li>• Advertise Route Map—Select the previously created route map that defines the path attributes for the aggregate route.</li> <li>• Attribute Route Map—Select the previously created route map that defines the route attributes for the aggregate route.</li> <li>• Suppress Route Map—Select the previously created route map that you want BGP to suppress for the aggregate route. If you select this option, you cannot enable Summary Only for this aggregate route.</li> </ul>

**Related Documentation**

- [BGP Overview on page 325](#)
- [Route-Refresh Capabilities Overview on page 326](#)
- [Configuring BGP Networks on page 327](#)
- [Configuring Neighbors and Peer Groups Overview on page 328](#)
- [Configuring a BGP Routing Instance \(NSM Procedure\) on page 329](#)

## Configuring Neighbors and Peer Groups Overview

Use the Neighbor settings to configure individual peer addresses, called neighbors. You can also assign neighbors to a *peer-group* to configure parameters for the peer-group as a whole (you cannot assign IBGP and EBGP peers to the same peer-group).

**Related Documentation**

- [BGP Overview on page 325](#)
- [Route-Refresh Capabilities Overview on page 326](#)
- [Configuring BGP Networks on page 327](#)
- [Configuring Aggregate Addresses on page 327](#)

## Configuring a BGP Routing Instance (NSM Procedure)

To configure BGP:

1. In the NSM navigation tree, select **Device Manager > Devices**. Double-click the device object to open the device configuration.
2. In the device navigation tree, select **Network > Virtual Router** to display the list of configured virtual routers. Double-click the virtual router in which you are configuring a BGP routing instance. The Virtual Router configuration screen appears.
3. In the virtual router navigation tree, select **Dynamic Routing Protocol** and enable **Configured BGP Instance** check box. BGP configuration options now appear in the virtual router navigation tree under Dynamic Routing Protocol.
4. In the virtual router navigation tree, select **BGP > Parameters** to display the Parameters screen. Configure the following:
  - Select the **Enable BGP** check box.
  - Enter an AS Number.
5. In the virtual router navigation tree, select **BGP > Neighbors** to display the Neighbors screen. Click the Add icon to display the New Neighbor screen. Configure the following:
  - Select the **Peer Enabled** check box.
  - Enter the BGP peer information.
6. Click **OK** to save the new neighbor.
7. Click **OK** to save your changes to the virtual router.
8. In the device navigation tree, select **Network > Interface** to display the list of interfaces. Double-click the interface that is connected to the BGP peer to open the interface screen.
9. In the interface navigation tree, select **Protocol** to display the Protocol screen, and then click the **BGP** tab and enable **BGP** check box.
10. Click **OK**.

### Related Documentation

- [BGP Overview on page 325](#)
- [Route-Refresh Capabilities Overview on page 326](#)
- [Multicast Route Overview on page 335](#)
- [Configuring Neighbors and Peer Groups Overview on page 328](#)
- [Configuring BGP Networks on page 327](#)
- [Configuring Aggregate Addresses on page 327](#)

## Configuring NHRP Overview

---

ScreenOS devices support autoconnect virtual private networks (ACVPNs) in a hub-and-spoke network topology. ACVPN provides a way for you to configure your hub-and-spoke network so that spokes can dynamically create VPN tunnels directly between each other as needed. This not only solves the problem of latency between spokes but also reduces processing overhead on the hub and thus improves overall network performance. Additionally, because ACVPN creates dynamic tunnels that time out when traffic ceases to flow through them, network administrators are freed from the time-consuming task of maintaining a complex network of static VPN tunnels.

After you set up a static VPN tunnel between the hub and each of the spokes, you configure ACVPN on the hub and the spokes and then enable the Next Hop Resolution Protocol (NHRP). The hub uses NHRP to obtain a range of information about each spoke, including its public-to-private address mappings, subnet mask length, and routing and hop count information, which the hub caches. Then, when any spoke begins communicating with another spoke (through the hub), the hub uses this information, in combination with information obtained from the ACVPN configuration on the spokes, to enable the spokes to set up an ACVPN tunnel between themselves. While the tunnel is being negotiated, communication continues to flow between the two spokes through the hub. When the dynamic tunnel becomes active, the hub drops out of the link and traffic flows directly between the two spokes. When traffic ceases to flow through the dynamic tunnel, the tunnel times out.

In cases where the hub fails and the dynamic tunnel expires, the spokes cannot reestablish the connection. To avoid this, ScreenOS 6.3 allows you to configure two hubs on the same virtual router (VR) so that connectivity is not lost even if one hub fails.

As ACVPN supports dynamic routing protocols, traffic from other subnets behind the spoke that needs to be routed through a hub may pass through the dynamic tunnel already created by the first cached subnet. To avoid this, ScreenOS 6.3 allows you to disable the dynamic routing operation on the ACVPN tunnel. Additionally, you can redistribute routes learned from NHRP into dynamic routing protocols such as BGP, OSPF, and RIP. In the same way, routes learned by the dynamic routing protocols can be redistributed automatically into the NHRP routing instance.

The following procedure explains how ACVPN works:

1. Adjust the topology to assign the VPN and gateway.
2. Assign the ACVPN—dynamic and next-hop server (NHS) IP address.
3. Set the NHRP redistribute rules.
4. Add NHRP to other dynamic routing protocols such as OSPF, BGP, and RIP redistribute.
5. Set the routing on tunnel interface.

You can configure the NHRP parameters as described in [Table 82 on page 331](#).

Table 82: NHRP Parameters

NHRP Parameters	Description
Enable	Enables the NHRP parameters.
Hold Time	Configures the number of seconds that NHRP waits before updating the routing table. Default is 300.
No of Query's before giveup	Specifies the attempts that a query updates the routing table.
Res-Req. Retry Interval	Ensures that the NHS has current information about its subnetworks by having the next-hop client (NHC) periodically send Resolution Request messages to the NHS at regular intervals. If any devices have been added to or removed from their subnetworks, that information is contained in the Resolution Request message, and the NHS updates its cache and retries at regular intervals.
ACVPN-Profile	Specifies the autoconnect virtual private network profile. Select any value from the drop-down list.
ACVPN-Dynamic	Specifies the autoconnect virtual private network dynamic routers. Select any value from the drop-down list.
NHS IP Address	Next hop server IP address in a hub-and-spoke network.
NHS IP Address 2	Next hop server IP address 2 in a hub-and-spoke network.

**Related  
Documentation**

- [BGP Overview on page 325](#)
- [Configuring Neighbors and Peer Groups Overview on page 328](#)
- [Configuring BGP Networks on page 327](#)
- [Configuring Aggregate Addresses on page 327](#)

## Configuring OSPFv3 Overview

This topic includes information on how to configure, monitor, and operate OSPFv3 implementations. This topic has the following sections:

- [OSPFv3 Support in Virtual Routers on page 331](#)
- [OSPFv3 Support in Interfaces on page 332](#)
- [OSPFv3 Area Parameters on page 332](#)
- [Redistribution Rules on page 332](#)
- [OSPFv3 Interface Parameters on page 332](#)
- [OSPFv3 Route Preference on page 333](#)

### OSPFv3 Support in Virtual Routers

In dynamic routing protocols, each virtual router (VR) in the security device uses a unique virtual router identifier (VRID) to communicate with other routing devices. The identifier

uses a dotted decimal notation, similar to an IP address, or an integer value. The router ID of the OSPFv3 instance is always equal to the VRID of the VR that it belongs to. Select **Virtual Router** > edit a VR > **Dynamic Routing Protocol**, and then select the **Configured OSPFv3 Instance** check box to configure a OSPFv3 instance.

## OSPFv3 Support in Interfaces

OSPFv3 is supported in tunnel interfaces. You can enable OSPFv3 on tunnel interfaces in the same way as any regular physical interface. By default, you can assign the tunnel as a point-to-point link OSPFv3. There must be at least one pure IPv6 IPsec or IPv6 over IPv4 IPsec VPN to make the two OSPFv3 routers at the end of the tunnel interface communicate adjacently. OSPFv3 is supported on all IPv6 physical interfaces.

## OSPFv3 Area Parameters

You can configure the following area parameters in an OSPFv3 area as described in [Table 83 on page 332](#).

**Table 83: OSPFv3 Area Parameters**

OSPFv3 Area Parameters	Description
Area range	Allows a group of subnets to be consolidated into a single network address. This range can be advertised in a single summary link advertisement to other areas. When you configure an area range, you can specify whether to advertise or withhold the defined area range in advertisements.
Metric of default route	Specifies the metric for the default route advertisement.
Filter out summary LSAs	Specifies that the summary link state advertisements (LSAs) are not advertised in the area.

## Redistribution Rules

Route redistribution is the exchange of route information between the routing protocols. Redistribution routes can be outlined based on the summary list or filtered based on the IPv6 enabled route-map. The IPv6 routes can be redistributed into the OSPFv3 routing instance in the same VR. You can also summarize the routers redistributed in **Dynamic Routing Protocol** > **OSPFv3** > **Summary Import**. You can also enhance Border Gateway Protocol (BGP) to redistribute OSPFv3 route. The OSPFv3 routes can be redistributed with RIPng also.

## OSPFv3 Interface Parameters

[Table 84 on page 332](#) describes the interface parameters in an OSPFv3 enabled interface that you can configure.

**Table 84: Interface Parameters**

Interface Parameters	Description
Cost	Specifies the metric for the interface. The cost associated with an interface depends upon the bandwidth of the link to which the interface is connected. The higher the bandwidth, the lower the cost value is.



Table 84: Interface Parameters (*continued*)

Interface Parameters	Description
Hello Interval (Secs)	Specifies the interval at which OSPFv3 sends out hello packets to the network.
Configure to ignore mtu mismatch in DB exchange	Specifies any mismatches in the maximum transmission unit (MTU) values between the local and remote interfaces that are found during OSPFv3 database negotiations are ignored.
Instance ID	Controls some of the other routers as your neighbors. You can become neighbors only with routers having same instance ID.
Interface Link Type	Specifies that OSPFv3 treats an interface as a point-to-point link or as a point-to-multipoint link.
Interface OSPFv3 Passive Mode	Specifies that the IP address of the interface is advertised into the OSPFv3 domain as an OSPFv3 route, but the interface does not transmit or receive OSPFv3 packets.
OSPFv3 Priority	Specifies the priority of the VR as a designated router or a backup designated router. The router with the larger priority value has the best chance (although not guaranteed) of being elected.
Retransmit Interval	Specifies the number of seconds that elapses before the interface resends an LSA to a neighbor that did not respond to the original LSA.
Transit Delay	Specifies the number of seconds between transmissions of link-state update packets sent to the interface.

## OSPFv3 Route Preference

OSPFv3 uses route preferences to select which route is installed in the forwarding table, when several protocols calculate routes to the same destination. The route with the lowest preference value is selected. For OSPFv3 and OSPFv3 External Type 2, select any value between 0 and 255.

### Related Documentation

- [Configuring NHRP Overview on page 330](#)
- [Configuring a BGP Routing Instance \(NSM Procedure\) on page 329](#)
- [Configuring RIPng Overview on page 334](#)

## Configuring RIPng Overview

Devices running ScreenOS 6.3 support static routing and dynamic routing with the Routing Information Protocol next-generation (RIPng), an interior gateway protocol (IGP) that uses a distance-vector algorithm to determine the best route to a destination, using the hop count as the metric. RIPng supports route redistribution to import known routes, from a router running a different protocol, into the current RIPng routing instance. For example, you can import static routes from a virtual router (VR) into a RIPng instance. RIPng is intended only for use in IPv6 networks. You can create RIPng on a per VR basis on a security device. If you have multiple VRs within a system, you can enable multiple instances of RIPng. OSPFv3 like RIPng is a new dynamic routing protocol that works on IPv6 interfaces.

To configure RIPng on a security device:

1. Create the RIPng routing instance in a VR.
2. Enable the RIPng instance.
3. Enable RIPng on interfaces that connect to other RIPng routers.
4. Redistribute routes learned from different routing protocols (such as OSPF, BGP, or statically configured routes) into the RIPng instance.

This topic describes the following RIPng options:

- [RIPng Parameters on page 334](#)
- [Redistribution Rules on page 335](#)

### RIPng Parameters

You can configure some global RIPng parameters at the VR level. When you configure a RIPng parameter at the VR level, the parameter setting affects operations on all RIPng-enabled interfaces. [Table 85 on page 334](#) describes the RIPng global parameters that you can configure.

**Table 85: Global RIPng Parameters and Default Values**

RIPng Global Parameter	Description	Default Description Value(s)
Advertising Default Route	Specifies whether the default route (::/0) is advertised.	Disabled
Default Metric	Specifies the default metric value for routes imported into RIPng from other protocols, such as OSPF and BGP.	10
Flush Timer	Specifies, in seconds, when a route is removed from the time the route becomes invalid	120 seconds
Invalid Timer	Specifies, in seconds, when a route becomes invalid from the time a neighbor stops advertising the route.	180 seconds

Table 85: Global RIPng Parameters and Default Values (*continued*)

RIPng Global Parameter	Description	Default Description Value(s)
Maximum Number of Neighbors Allowed on One Interface	Specifies the maximum number of RIPng neighbors allowed.	256
Reject Default Route	Specifies whether RIPng rejects a default route learned from another protocol.	Disabled
Inbound Route Map	Specifies the filter for routes to be learned by RIPng.	None. Select a value from the drop-down list.
Outbound Route Map	Specifies the filter for routes to be advertised by RIPng.	None. Select a value from the drop-down list.
Access List Number To Filter Only Trusted Neighbors	Specifies an access list that defines RIPng neighbors. If no neighbors are specified, the RIPng uses multicasting or broadcasting to detect neighbors on an interface.	None. All neighbors are trusted.
Update Timer	Specifies, in seconds, when to issue updates of RIPng routes to neighbors.	30 seconds

## Redistribution Rules

Redistribution rules exchange route information between routing protocols. You need to configure a route map to filter the routes that are redistributed. Routes imported into RIPng from other protocols have a default metric of 10. You can change the default metric.

You can redistribute the following types of rules into the RIPng routing instance in the same VR:

- Routes learned from BGP
- Routes learned from OSPF
- Directly connected routes
- Imported routes
- Statically configured routes

### Related Documentation

- [Configuring NHRP Overview on page 330](#)
- [Configuring a BGP Routing Instance \(NSM Procedure\) on page 329](#)

## Multicast Route Overview

Multicast routing environments require the following items:

- A mechanism between hosts and routers to communicate group membership information. Security devices support the Internet Group Management Protocol (IGMP) versions 1, 2, and 3.
- A multicast routing protocol to populate the multicast route table and forward multicast traffic to hosts throughout the network. Security devices support the Protocol Independent Multicast-Sparse Mode (PIM-SM) protocol. Alternatively, you can use IGMP proxy to transmit multicast information between routers without the CPU overhead of a multicast routing protocol



**NOTE:** Multicast routing is only supported in ScreenOS 5.1 and later.

This topic describes the basic steps to configure the following multicast protocols:

- [Configuring IGMP \(NSM Procedure\) on page 336](#)
- [Configuring IGMP Proxy \(NSM Procedure\) on page 337](#)
- [Configuring PIM Sparse Mode \(NSM Procedure\) on page 339](#)



**NOTE:** The NSM UI displays the multicast parameters and multicast static routes that you configure. It does not display dynamic information about multicast protocols at the device level. (For example, whether or not an interface is a querier in IGMP.) For this information, you must issue the appropriate CLI get commands from the device.

**Related  
Documentation**

- [RIP Overview on page 319](#)
- [BGP Overview on page 325](#)

---

## Configuring IGMP (NSM Procedure)

On security devices, you must explicitly enable IGMP in Router mode on the interfaces that are connected to hosts. Security devices support the following Internet Group Management Protocol (IGMP) versions:

- IGMPv1, as defined in RFC 1112, *Host Extensions for IP Multicasting*, defines the basic operations for multicast group memberships.
- IGMPv2, as defined in RFC 2236, *Internet Group Management Protocol, Version 2*, expands on the functionality of IGMPv1.
- IGMPv3, as defined in RFC 3376, *Internet Group Management Protocol, Version 3*, adds support for source filtering. Hosts running IGMPv3 indicate which multicast groups they want to join and the sources from which they expect to receive multicast traffic. IGMPv3 is required when you run Protocol Independent Multicast in source-specific multicast (PIM-SSM) mode.

To enable IGMP in Router mode:

1. In the NSM navigation tree, select **Device Manager > Devices**. Double-click the device object to open the device configuration.
2. In the device navigation tree, select **Network > Interface**.
3. Double-click the interface on which you are enabling IGMP. The General Properties screen appears.
4. In the interface navigation tree, select **Protocol**.
5. Select the **IGMP** tab and configure the following options:
  - In the Type box, select **Router**.
  - Select **Enable**.
  - Click **OK** to save your changes to the interface.
6. Click **OK** to save your changes to the device.

You can optionally change the default parameters for each interface on which IGMP is enabled. You can also use access lists to control traffic to and from an IGMP interface. First, create access lists that identify the following items:

- Multicast groups that the hosts on a specified interface can join
- Hosts from which an IGMP router interface can receive IGMP messages
- Routers that are eligible for querier selection

Then, enter the access list IDs in the IGMP configuration screen of the IGMP interface(s). The security device then filters IGMP traffic based on the access lists.

#### Related Documentation

- [RIP Overview on page 319](#)
- [BGP Overview on page 325](#)
- [Multicast Route Overview on page 335](#)
- [Configuring IGMP Proxy \(NSM Procedure\) on page 337](#)
- [Configuring PIM Sparse Mode \(NSM Procedure\) on page 339](#)

## Configuring IGMP Proxy (NSM Procedure)

IGMP proxy enables a security device to extend the scope of a multicast domain by one hop without running a multicast routing protocol. When you enable IGMP proxy on a device, the interface connected to the hosts (downstream interface) functions as a multicast router, and the interface connected to the upstream router functions as an IGMP host. You must first enable IGMP in host mode on upstream interfaces, and then enable IGMP in Router mode on downstream interfaces, and finally enable IGMP proxy on router interfaces.

To configure an IGMP proxy:

1. In the NSM navigation tree, select **Device Manager > Devices**. Double-click the device object to open the device configuration.
2. In the device navigation tree, select **Network > Interface**.
3. Double-click the interface on which you are enabling IGMP. The General Properties screen appears.
4. In the interface navigation tree, select **Protocol**.
5. Select **IGMP**.
  - If you are enabling IGMP on an upstream interface:
    - In the Type box, select **Host**.
    - Select **Enable**.
  - If you are enabling IGMP on a downstream interface:
    - In the Type box, select **Router**.
    - Select **Enable**.
    - Select **Proxy**.
  - Click **OK** to save your changes to the routing entry.
  - Click **OK** to save your changes to the device.

After you configure the interfaces, configure a multicast rule to permit IGMP messages to pass between zones. For information about multicast rules, see the *Network and Security Manager Administration Guide*.

**Related  
Documentation**

- [RIP Overview on page 319](#)
- [BGP Overview on page 325](#)
- [Multicast Route Overview on page 335](#)
- [Configuring IGMP \(NSM Procedure\) on page 336](#)
- [Configuring PIM Sparse Mode \(NSM Procedure\) on page 339](#)
- [Configuring a Rendezvous Point to Group Mappings \(NSM Procedure\) on page 340](#)

## Configuring PIM Sparse Mode (NSM Procedure)

To configure PIM sparse mode (PIM-SM) in a virtual router on a security device:

1. Configure either a static route or a dynamic routing protocol, such as OSPF. (For information about configuring static routes, see [“Routing Table Entries Overview” on page 303](#). For information about dynamic routing protocols, see [“Dynamic Routing Configuration Overview” on page 311](#).)
2. Create a security policy to pass unicast and multicast data traffic between zones. (For details on security policies, see the *Network and Security Manager Administration Guide*.)
3. Create and enable the PIM-SM routing instance in a virtual router.
4. Select PIM-SM on interfaces that transmit multicast traffic.
5. Configure a multicast rule to permit PIM-SM messages between zones. (For details on multicast rules, see the *Network and Security Manager Administration Guide*.)

After you enable the PIM-SM routing instance in the virtual router and enable it on all applicable interfaces, you can optionally configure PIM-SM features such as the following:

- Use access lists to restrict the rendezvous points (RPs) and sources from which a multicast group can receive traffic. You can also use access lists to restrict the multicast groups for which the virtual router forwards PIM join-prune messages. First, create the access lists, and then enter the access list IDs in the PIM-SM configuration screen of the virtual router. The security device then uses the access lists to filter the PIM-SM traffic.
- Change the default parameters for each interface on which PIM-SM is enabled. When you set parameters at this level, the parameters affect the specific interface only.
- Configure a static RP for a particular zone, or use dynamic RP mappings and configure a virtual router as a candidate rendezvous point (C-RP).
- You can configure a virtual router to function as a proxy RP.

To configure PIM-SM:

1. In the NSM navigation tree, select **Device Manager > Devices**. Double-click the device icon to open the device configuration.
2. Configure the virtual router for PIM-SM:
  - In the device navigation tree, select **Network > Virtual Router**.
  - Double-click the virtual router in which you are configuring a PIM-SM instance. The General Properties screen appears.
  - In the virtual router navigation tree, select **Dynamic Routing Protocol**.
  - Select **Configure PIM-SM**. PIM-SM configuration options now appear in the virtual router navigation tree under Dynamic Routing Protocol.

- In the virtual router navigation tree, select **Dynamic Routing Protocol > PIM-SM > Parameters**. The Parameters configuration screen appears.
  - Select **Enable** in the main display area,
  - Click **OK** to save your changes to the virtual router.
3. Configure the interface for PIM-SM:
    - In the device navigation tree, select **Network > Interface**.
    - Double-click the interface that transmits multicast traffic. The General Properties screen appears.
    - In the interface navigation tree, select **Protocol**, and then select the **PIM-SM** tab in the main display area.
    - Select **Configure PIM-SM on Interface**.
    - Select **Enable PIM-SM**.
    - Click **OK** to save your changes to the interface. Repeat Step 3 to enable PIM-SM on additional interfaces.
  4. Click **OK** to save your changes to the device configuration.

**Related Documentation**

- [RIP Overview on page 319](#)
- [BGP Overview on page 325](#)
- [Multicast Route Overview on page 335](#)
- [Configuring IGMP \(NSM Procedure\) on page 336](#)
- [Configuring IGMP Proxy \(NSM Procedure\) on page 337](#)
- [Configuring a Rendezvous Point to Group Mappings \(NSM Procedure\) on page 340](#)

---

## Configuring a Rendezvous Point to Group Mappings (NSM Procedure)

---

You can configure a static rendezvous point (RP) for a particular zone and/or configure a virtual router as a candidate RP (C-RP). Before you configure a static RP and a C-RP, you must first create access lists that identify the multicast groups mapped to each one.

To configure an RP:

1. In the NSM navigation tree, select **Device Manager > Devices**. Double-click the device icon to open the device configuration.
2. Configure the virtual router for PIM-SM:
  - In the device navigation tree, select **Network > Virtual Router**.
  - Double-click the virtual router in which you are configuring a PIM-SM instance. The General Properties screen appears.
  - In the virtual router navigation tree, select **Dynamic Routing Protocol**.



- Select the **Configure PIM-SM** check box. PIM-SM configuration options now appear in the virtual router navigation tree under Dynamic Routing Protocol.
  - In the virtual router navigation tree, select **Dynamic Routing Protocol > PIM-SM > Rendezvous Points**.
  - Click the Add icon. The new Zone dialog box appears. For Zone, select the zone that contains the RP.
3. Configure a C-RP:
    - Select the interface that is advertised as the C-RP.
    - Specify the access list that identifies the multicast group(s) for which the interface is the RP candidate.
    - Select the advertised C-RP priority.
    - Select the holdtime advertised to the bootstrap router.
  4. Configure a static rendezvous point:
    - Click the Add icon in the Static RP Addresses area. The Static RP Addresses dialog box appears.
    - Enter the IP address of the RP.
    - Specify the access list that identifies the multicast group(s) mapped to the RP.
    - If you want to always use the same RP for the specified multicast group(s), select the **Always used as RP** check box. Use this option to override dynamic group-RP mappings.
  5. Click **OK** to save your changes to the virtual router, and then click **OK** to save your changes to the device configuration.

**Related  
Documentation**

- [Access List Overview on page 296](#)
- [Multicast Route Overview on page 335](#)
- [Configuring IGMP \(NSM Procedure\) on page 336](#)
- [Configuring IGMP Proxy \(NSM Procedure\) on page 337](#)
- [Configuring PIM Sparse Mode \(NSM Procedure\) on page 339](#)
- [Configuring Acceptable Groups \(NSM Procedure\) on page 341](#)

## Configuring Acceptable Groups (NSM Procedure)

You can create access lists to identify the acceptable sources, multicast groups, and RPs, and then configure the virtual router to accept PIM messages only from those specified in the access lists.

To configure acceptable groups on the virtual router:

1. In the NSM navigation tree, select **Device Manager > Devices**. Double-click the device icon to open the device configuration.
2. Configure the virtual router for PIM-SM:
  - In the device navigation tree, select **Network > Virtual Router**.
  - Double-click the virtual router in which you are configuring a PIM-SM instance. The General Properties screen appears.
  - In the virtual router navigation tree, select **Dynamic Routing Protocol**.
  - Select the **Configure PIM-SM** check box. PIM-SM configuration options now appear in the virtual router navigation tree under Dynamic Routing Protocol.
  - In the virtual router navigation tree, select **Dynamic Routing Protocol > PIM-SM > Acceptable Groups**.
  - Select the access list that identifies the permitted multicast group(s).
  - In the Group Specific Access Policies area, click the Add icon to map a multicast group to access lists. The Multicast Group IP dialog box appears.
  - Enter the IP address of the multicast group for which you created access lists for permitted RPs and permitted sources.
  - Select the ID of the access list that identifies the permitted RP(s). The device drops traffic for the multicast group if the traffic is from an RP that is not on the access list.
  - Select the ID of the access list that identifies the permitted source(s). This prevents unauthorized sources from sending data into your network. When you use this feature, the device drops multicast data from sources not in the list.
3. Click **OK** to save the new Multicast Group IP.
4. Click **OK** to save your changes to the virtual router, and then click **OK** again to save your changes to the device configuration.

**Related  
Documentation**

- [Access List Overview on page 296](#)
- [RIP Overview on page 319](#)
- [Multicast Route Overview on page 335](#)
- [Configuring a Rendezvous Point to Group Mappings \(NSM Procedure\) on page 340](#)
- [Example: Configuring Proxy RP on page 342](#)

---

## Example: Configuring Proxy RP

You can configure a virtual router to function as a proxy rendezvous point (RP). A proxy RP acts as the RP for groups learned from other zones. To configure a virtual router as a proxy RP, select **Proxy** when configuring the RP for PIM-SM.

In this example, the hosts in the Trust zone are to receive the multicast stream for the multicast group 224.4.4.1/32. You configure RIP as the unicast routing protocol and create a firewall rule to pass data traffic between the Trust and Untrust zones. You create a PIM instance on the trust-vr and enable PIM on ethernet1 in the Trust zone, and on ethernet2 in the Untrust zone. ethernet1 is connected to the potential receivers; so, you also configure IGMP in router mode on this interface. You then create a multicast rule that permits PIM-SM BSR and join-prune messages between the zones.

To configure proxy RP:

1. Configure zones and interfaces.
  - Configure ethernet1 and bind it to the Trust zone.
  - Select IGMP in router mode on ethernet1.
  - Configure ethernet2 and bind it to the Untrust zone.
2. Configure the following address objects:
  - Multicast group IP address.
  - Source IP address
  - Configure the access list that permits traffic from multicast group 224.4.4.
3. Configure RIP.
  - Create a RIP instance on the trust-vr.
  - Select RIP on ethernet1 and on ethernet3.
4. Configure PIM-SM.
  - Create a PIM-SM instance on the trust-vr.
  - Select **Enable** in the Parameters screen.
  - Select PIM-SM on ethernet1 and on ethernet3.
5. Configure a firewall rule that permits unicast and multicast data traffic to pass between zones.
6. Configure a multicast rule permitting PIM-SM messages to pass between zones

#### Related Documentation

- [Access List Overview on page 296](#)
- [RIP Overview on page 319](#)
- [Multicast Route Overview on page 335](#)
- [Multicast Routing Table Entries Overview on page 344](#)
- [Configuring a Rendezvous Point to Group Mappings \(NSM Procedure\) on page 340](#)
- [Configuring Acceptable Groups \(NSM Procedure\) on page 341](#)

## Multicast Routing Table Entries Overview

---

Use static multicast routes to forward multicast data from hosts on interfaces in IGMP router proxy mode to routers upstream on the interfaces in IGMP host mode. (For information about IGMP proxy, see [“Configuring IGMP Proxy \(NSM Procedure\)” on page 337](#)).

**Related  
Documentation**

- [Multicast Route Overview on page 335](#)
- [Multicast Routing Table Preferences Overview on page 344](#)

## Multicast Routing Table Preferences Overview

---

You can configure the following settings for the multicast routing table:

- **Enable Multiple Incoming Interfaces**—Select this option to permit multiple routes with different incoming interfaces for the same source and multicast group.
- **Maximum Entries**—Enter the maximum number of route entries you want the multicast routing table to hold. By default, this option is set to 4096.
- **Negative Mroute Cache**—Select this option to store unrouteable multicast packets in a cache until a multicast route can be established for the packet. For example, the security device might be unable to immediately route a multicast packet when:
  - The IGMP proxy receives a data packet for which it has no interested member. The device creates a negative mroute entry for the packet and stores the packet in the negative mroute cache. When the IGMP proxy receives a group join for the source (or source and group), the device automatically forwards the cached packet.
  - The device receives a data packet from a locally connected PIM-SM but does not have a group RP mapping for that group. The device creates a negative mroute entry for the packet and stores the packet in the negative mroute cache. When the device learns the RP mapping, it automatically registers and forwards the packet.
  - In an active-active NSRP configuration, the device that is not responsible for forwarding packets receives a multicast data packet. The device creates a negative mroute entry for the packet and stores the packet in the negative mroute cache. When the device that is responsible for forwarding packets learns of the group interest for the data packet, it forwards the packet.

When you enable Negative Mroute Cache, you can also configure a timer that controls how the device ages unrouteable packets in the cache. By default, the timer is set to 90 seconds, meaning that the device deletes a route entry in the cache after 90 seconds. The acceptable range is 10 to 180 seconds.

**Related  
Documentation**

- [Multicast Route Overview on page 335](#)
- [Multicast Routing Table Entries Overview on page 344](#)
- [Configuring Multicast Static Routes on page 345](#)

## Configuring Multicast Static Routes

For each static entry in the multicast routing table, you must configure the following information:

- Multicast Group IP—Enter the IP address of the group that receives multicast traffic.
- Source IP—Enter the IP address of the source of the multicast traffic.
- Incoming Interface—Select the interface on the device that receives multicast traffic.
- Outgoing Information—Enter the information that defines the interface and IP address the device uses to forward multicast traffic.
  - Outgoing Interface—Select the interface on the device that forwards multicast traffic.
  - Outgoing Group—Security devices can translate the original multicast group address to a different multicast group address on the outgoing interface. Use this option to specify the translated multicast group address for the outgoing interface (you configure the original group address in the Multicast Group IP setting).

### Related Documentation

- [Multicast Route Overview on page 335](#)
- [Multicast Routing Table Entries Overview on page 344](#)
- [Multicast Routing Table Preferences Overview on page 344](#)
- [Configuring IGMP \(NSM Procedure\) on page 336](#)
- [Configuring IGMP Proxy \(NSM Procedure\) on page 337](#)
- [Example: Configuring Multicast Static Routes \(NSM Procedure\) on page 345](#)

## Example: Configuring Multicast Static Routes (NSM Procedure)

You can configure multiple Outgoing Information settings for a single static multicast route.

In this example, you configure a static multicast route from a source with IP address 20.20.20.200 to the multicast group 238.1.1.1. You configure the security device to translate the multicast group from 238.1.1.1 to 238.2.2.1 on the outgoing interface.

To configure a multicast static route:

1. In the navigation tree, select **Device Manager > Devices**. Double-click the device object to open the device configuration.
2. In the device navigation tree, select **Network > Virtual Router** to display the list of configured virtual routers. Double-click the virtual router in which you are configuring a static multicast routing entry. The Virtual Router configuration screen appears.
3. In the virtual router navigation tree, select **Multicast Routing Table**. Configure the multicast routing preferences:
  - Select **Enable Multiple Incoming Interfaces**.

- Select the **Negative Mroute Cache**. Leave the default Timer setting of 4096.
4. In the Multicast Static Routes area, click the Add icon. The New Mgroup dialog box appears. Configure the new routing entry:
    - For Multicast Group IP, enter **238.1.1.1**.
    - For Source IP, enter **20.20.20.200**.
    - For Incoming Interface, select **ethernet1**.
  5. Configure an Outgoing Information setting:
    - Click the Add icon. The New Outgoing Information dialog box appears.
    - For outgoing interface, select **ethernet3**.
    - For Outgoing Group, enter the IP address **238.2.2.1**.
  6. Click **OK** to add the Outgoing Information setting to the static route settings. Repeat step 5 to add more Outgoing Information settings.
  7. Click **OK** to save your changes to the virtual router, and then click **OK** again to save your changes to the device.

**Related Documentation**

- [Multicast Route Overview on page 335](#)
- [Multicast Routing Table Entries Overview on page 344](#)
- [Multicast Routing Table Preferences Overview on page 344](#)
- [IRDP Support Overview on page 346](#)
- [Configuring IGMP \(NSM Procedure\) on page 336](#)
- [Configuring IGMP Proxy \(NSM Procedure\) on page 337](#)
- [Configuring Multicast Static Routes on page 345](#)

---

## IRDP Support Overview

ICMP Router Discovery Protocol (IRDP) is an ICMP message exchange between a host and a router. The security device is the router and advertises the IP address of a specified interface periodically or on demand. If the host is configured to listen, you can configure the security device to send periodic advertisements. If the host explicitly sends router solicitations, you can configure the security device to respond on demand.

Before a host can send IP datagrams beyond its directly connected subnet, it must discover the address of at least one operational router on that subnet. IRDP is a router discovery method that uses a pair of ICMP messages for use on multicast links. The messages are called router advertisements (RA) and router solicitations (RS). Each router periodically multicasts an RA from each of its multicast interfaces, announcing the IP address(es) of that interface. Hosts discover routers simply by listening for advertisements. The host may send out router solicitation messages seeking immediate advertisements at startup, rather than wait for periodic updates.



**NOTE:** ICMP Router Discovery Protocol (IRDP) is supported on all devices running ScreenOS 6.3, including the SSG520.

#### Related Documentation

- [Multicast Route Overview on page 335](#)
- [Multicast Routing Table Entries Overview on page 344](#)
- [Multicast Routing Table Preferences Overview on page 344](#)
- [Example: Configuring Multicast Static Routes \(NSM Procedure\) on page 345](#)
- [Example: Configuring ICMP Router Discovery Protocol \(NSM Procedure\) on page 347](#)

### Example: Configuring ICMP Router Discovery Protocol (NSM Procedure)

You can enable and disable IRDP and configure or view IRDP settings using NSM. When you enable IRDP on an interface, NSM initiates an immediate IRDP advertisement to the network. For information about configuring an interface, see the *Network and Security Manager Administration Guide*.

To configure IRDP for the trust interface:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Select a security device and then double-click the device on which you want to define forced timeout. The device configuration appears.
3. In the device navigation tree, select **Network > Interface**.
4. Select a trust interface, and click **Edit**.
5. In the interface navigation tree, select **Protocol** and select the **IRDP** tab.
6. Select the **Enable IRDP** check box.
7. Click **OK** to apply the settings.

[Table 86 on page 347](#) lists the IRDP parameters, default values, and available settings.

**Table 86: IRDP Protocol Settings**

IRDP Parameters	Default Values	Available Settings
IPv4 address	<ul style="list-style-type: none"> <li>• Primary and secondary IP addresses—advertised</li> <li>• Management and webauth IP addresses—not advertised</li> </ul>	Advertise—you can add a preference value (-1through 2147483647)
Broadcast Advertisement	Disabled	Enabled
Init Advertise Interval after Enable	16 seconds	1 through 32 seconds
Init Advertise Packet Count	3	1 through 5

Table 86: IRDP Protocol Settings (*continued*)

IRDP Parameters	Default Values	Available Settings
Lifetime	Three times the Max Advertise Interval value	Max Advertise Interval value through 9000 seconds
Max Advertise Interval	600 seconds	4 through 1800 seconds
Min Advertise Interval	75% of the Max Advertise Interval value	3 through Max Advertise Interval value
Response Delay	2 seconds	0 through 4 seconds

#### Related Documentation

- [Multicast Route Overview on page 335](#)
- [Multicast Routing Table Entries Overview on page 344](#)
- [Multicast Routing Table Preferences Overview on page 344](#)
- [IRDP Support Overview on page 346](#)
- [Disabling IRDP on page 348](#)
- [Example: Configuring Multicast Static Routes \(NSM Procedure\) on page 345](#)

## Disabling IRDP

You can disable an interface from running IRDP; however, when you do so, ScreenOS deletes all related memory from the original configuration.

To disable the Trust interface from running IRDP, enter the following command:

```
unset interface trust protocol irdp enable
```



**NOTE:** For details on viewing IRDP information from the Web UI or the CLI, see the *Concepts & Examples ScreenOS Reference Guide*.

#### Related Documentation

- [Multicast Route Overview on page 335](#)
- [Multicast Routing Table Entries Overview on page 344](#)
- [Multicast Routing Table Preferences Overview on page 344](#)
- [IRDP Support Overview on page 346](#)
- [Example: Configuring Multicast Static Routes \(NSM Procedure\) on page 345](#)
- [Example: Configuring ICMP Router Discovery Protocol \(NSM Procedure\) on page 347](#)



## Policy-Based Routing Overview

Policy-based routing (PBR) provides a flexible mechanism for forwarding data packets based on policies configured by a network administrator. PBR enables you to implement policies that selectively cause packets to take different paths. PBR provides a routing mechanism for networks that rely on Application Layer support, such as antivirus (AV), deep inspection (DI), or antispam, Web filtering, and/or that require an automatic way to specific applications.

When a packet enters the security device, ScreenOS checks for PBR as the first part of the route-lookup process, and the PBR check is transparent to all non-PBR traffic. PBR is enabled at the interface level and configured within a virtual router context; but you can choose to bind PBR policies to an interface, a zone, a virtual router (VR), or a combination of interface, zone, or VRs.

You use the following three building blocks to create a PBR policy:

- Extended access lists—Extended access-lists list the match criteria you define for PBR policies.
- Match groups—Match groups provide a way to organize (by group, name and priority) extended access lists.
- Action groups—Action groups specify the route that you want a packet to take. You specify the “action” for the route by defining the next interface, the next-hop, or both.



**NOTE:** For details on configuring policy-based routing and route lookup, see the *Concepts & Examples ScreenOS Reference Guide*.

### Related Documentation

- [Configuring Virtual Routers on page 292](#)
- [Virtual Router General Properties Overview on page 295](#)
- [Access List Overview on page 296](#)
- [Route Map Overview on page 298](#)
- [IRDP Support Overview on page 346](#)
- [Example: Configuring Access Lists \(NSM Procedure\) on page 297](#)
- [Example: Configuring Policy-Based Routing \(NSM Procedure\) on page 349](#)

## Example: Configuring Policy-Based Routing (NSM Procedure)

To configure policy-based routing for a security device:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Select a security device and then double-click the device on which you want to define forced timeout. The device configuration appears.

3. In the device navigation tree, select **Network > Virtual Router**.
4. Click **New** to view the configuration page.
5. In the virtual router navigation tree, select access list and configure the options for access list 10:
  - Extended ACL ID: **10**
  - Sequence Number: **1**
  - Source IP Address/Netmask: **172.18.1.10/32**
  - Destination Port: **80-80**
  - Protocol: **TCP**
  - Click **OK** to return to the access lists.
6. Click **New** to configure a second entry for access list 10 and configure the following options:
  - Extended ACL ID: **10**
  - Sequence Number: **2**
  - Source IP Address/Netmask: **172.18.2.10/32**
  - Destination Port: **443-443**
  - Protocol: **TCP**
7. In the virtual router navigation tree, select **Policy-based**, and click **New** in the Match Group tab to configure the match group:
  - Match Group Name: **left\_router**
  - Sequence Number: **1**
  - Extended **ACL**: Select **10** from the drop down list.
8. In the virtual router navigation tree, select **Policy-based**, and click **New** in the Action Group tab to view the configuration page.
9. In the virtual router navigation tree, select **Policy-based**, and click **New** in the Policy tab to view the configuration page. Each PBR policy needs to have a unique name.
10. Use the policy binding tabs in the configuration page to bind policies.

**Related  
Documentation**

- [Configuring Virtual Routers on page 292](#)
- [Virtual Router General Properties Overview on page 295](#)
- [Access List Overview on page 296](#)
- [Route Map Overview on page 298](#)
- [IRDP Support Overview on page 346](#)
- [Policy-Based Routing Overview on page 349](#)
- [Disabling IRDP on page 348](#)

- [Example: Configuring Access Lists \(NSM Procedure\) on page 297](#)



## CHAPTER 11

# Virtual Systems

You can logically partition a single Juniper Networks security system into multiple virtual systems to provide multi-tenant services. Each virtual system (vsys) is a unique security domain and can have its own administrators (called virtual system administrators or vsys admins) who can individualize their security domain by setting their own address books, user lists, custom services, VPNs, and policies. Only a root-level administrator, however, can set firewall security options, create virtual system administrators, and define interfaces and subinterfaces.



**NOTE:** Refer to the Juniper Networks marketing literature to see which platforms support this feature.

Juniper Networks virtual systems support two kinds of traffic classifications: VLAN-based and IP-based, both of which can function exclusively or concurrently. For more information on how to create and view Vsys profiles and other resource information, see the *Concepts & Examples ScreenOS Reference Guide*.

This chapter contains the following topics:

- [Vsys DHCP Enhancement Overview on page 353](#)
- [Vsys Limitations Overview on page 354](#)
- [Example: Configuring Vsys Resource Limits \(NSM Procedure\) on page 355](#)
- [Vsys Session Limit Overview on page 356](#)
- [Example: Configuring Vsys Session Limit \(NSM Procedure\) on page 356](#)
- [Vsys CPU Limit Overview on page 357](#)
- [Example: Configuring CPU Limit \(NSM Procedure\) on page 358](#)

## Vsys DHCP Enhancement Overview

---

Dynamic Host Configuration Protocol (DHCP) was designed to reduce the demands on network administrators by automatically assigning the TCP/IP settings for the hosts on a network. Instead of requiring administrators to assign, configure, track, and change (when necessary) all the TCP/IP settings for every machine on a network, DHCP does it all automatically. Furthermore, DHCP ensures that duplicate addresses are not used,

reassigns unused addresses, and automatically assigns IP addresses appropriate for the subnet on which a host is connected.

NSM allows you to configure DHCP message relay from one or multiple DHCP servers to clients within a virtual system (vsys). You can configure DHCP message relay on an interface that is available to a virtual system.

If you have two DHCP servers, server 1 and server 2, a security device, sitting between the DHCP servers and a client, individually passes DHCP requests to each DHCP server on different outgoing interfaces. As each DHCP reply is received, the security device passes them to the root vsys and then forwards them to the appropriate DHCP client within a vsys.

To configure DHCP with vsys:

1. Create a vsys.
2. Enable DHCP for that vsys.
3. Configure a static route to allow the DHCP server in the root system to access the vsys.
4. Set security policies in the vsys.

For more details on DHCP server configuration and settings, see the *Concepts & Examples ScreenOS Reference Guide*.

**Related  
Documentation**

- [Virtual Routers Overview on page 294](#)
- [Virtual Router General Properties Overview on page 295](#)
- [Access List Overview on page 296](#)
- [Policy-Based Routing Overview on page 349](#)
- [Vsys Limitations Overview on page 354](#)
- [Vsys Session Limit Overview on page 356](#)

---

## Vsys Limitations Overview

The global maximum value for any vsys resource is dependent on the security device. If you do not explicitly set maximum and reserved limits, the default values for the device are used.

When setting maximum and reserved limits for resources, keep the following in mind:

- You cannot set the maximum value higher than the device-dependent global maximum value.
- For all resources except sessions, you cannot set the maximum value lower than the resources currently being used (actual-use value).

- You cannot set the reserved value higher than the configured maximum value.
- The total allocated usage, which is the sum of reserved values or actual-use values (whichever is higher) for all virtual systems, cannot exceed the global maximum value.



**NOTE:** For more information on setting vsys limitations, see the *Concepts & Examples ScreenOS Reference Guide*.

**Related Documentation**

- [Virtual Routers Overview on page 294](#)
- [Virtual Router General Properties Overview on page 295](#)
- [Access List Overview on page 296](#)
- [Policy-Based Routing Overview on page 349](#)
- [Vsys DHCP Enhancement Overview on page 353](#)
- [Vsys Session Limit Overview on page 356](#)

---

## Example: Configuring Vsys Resource Limits (NSM Procedure)

To configure vsys resource limits:

1. In the NSM navigation tree, select **Object Manager > VSYS Profile**.
2. Select the **Add** icon and configure the following options in the New VSYS Profile dialog box:
  - In the Name box, enter **Gold**.
  - For Scale-Size, Maximum, enter **32**.
  - For DIP enter **25** (Maximum) and **5** (Reserved).
  - For MIP enter **25** (Maximum).
  - For Policy enter **50** (Maximum).
  - For Mpolicy enter **5** (Maximum).
  - For Session Limitation enter **1200** (Maximum).
  - For CPU Weight, enter: **30**. The default is 50.
3. Click **OK** to apply the settings.

**Related Documentation**

- [Virtual Routers Overview on page 294](#)
- [Virtual Router General Properties Overview on page 295](#)
- [Access List Overview on page 296](#)
- [Policy-Based Routing Overview on page 349](#)
- [Vsys DHCP Enhancement Overview on page 353](#)

- [Vsys Limitations Overview on page 354](#)
- [Vsys Session Limit Overview on page 356](#)

## Vsys Session Limit Overview

The session limits that can be configured for a vsys are displayed in [Table 87 on page 356](#):

**Table 87: Vsys Session Limit Configuration Details**

Parameters	Description
session max	The session maximum is a number between 100 and the maximum session number for the overall security system. The default value is the maximum session number for the overall security system (as if no session limitation is in force).
reserve	In case of over-subscription, the reserve number is the number of sessions you reserve or guarantee for the specified vsys. The reserve value is a number between zero (0) and the maximum number of sessions you allocate for the specified vsys.
alarm	The alarm threshold is a percentage of the maximum limit that triggers the alarm. The default value is 100% of the session limit for a configured vsys.

### Related Documentation

- [Virtual Routers Overview on page 294](#)
- [Virtual Router General Properties Overview on page 295](#)
- [Access List Overview on page 296](#)
- [Policy-Based Routing Overview on page 349](#)
- [Vsys DHCP Enhancement Overview on page 353](#)
- [Vsys Limitations Overview on page 354](#)

## Example: Configuring Vsys Session Limit (NSM Procedure)

To configure the vsys session limit:

1. In the NSM navigation tree, select **Object Manager > VSYS Profile**.
2. Select **Vsys Profile Gold** (from previous example) and click **Edit**.
3. Configure as follows:
  - For Session Limitation enter **2500** (Maximum) and 2000 (Reserved).
  - For Alarm, enter **90** (indicates the alarm triggers when 90% of the session maximum is achieved).
  - Click **OK** to apply the settings.



- Related Documentation**
- [Vsys DHCP Enhancement Overview on page 353](#)
  - [Vsys Limitations Overview on page 354](#)
  - [Vsys Clusters Overview on page 376](#)
  - [Vsys Session Limit Overview on page 356](#)
  - [Vsys CPU Limit Overview on page 357](#)
  - [Example: Configuring Vsys Resource Limits \(NSM Procedure\) on page 355](#)

---

## Vsys CPU Limit Overview

By default, virtual systems within a single security system share the same CPU resources. It is possible for one virtual system (vsys) to consume excess CPU resources at the expense of other virtual systems.

For example, if one virtual system, within a security system that houses 20 virtual systems, experiences a DOS attack that consumes all of the CPU resources, the CPU is unable to process traffic for any of the other 19 virtual systems. In essence, all 20 virtual systems experience the DOS attack. CPU overutilization protection, also known as the CPU limit feature, is intended to protect against this.

Overutilization protection allows you to configure the security device for “fair use,” or fair mode, as opposed to “shared use,” or shared mode. To enable a fairer distribution of processing resources, you can assign a flow CPU utilization threshold to trigger a transition to fair mode, and you can choose a method for transition back to shared mode. By default, the security device operates in shared mode.

To enforce fair use, you assign a CPU weight to each vsys that you configure. ScreenOS uses these weights, relative to the weights of all virtual systems in the security device to assign time quotas proportional to those weights. ScreenOS then enforces the time quotas over one second intervals. This means that as long as a vsys does not exceed its time quota over that one second period and the firewall is not too heavily loaded, no packets for that vsys should be dropped.



**NOTE:** The CPU overutilization protection feature is independent of the session limits imposed by a vsys profile.

---

As system administrator, you determine how much traffic passes through a given vsys in fair mode by setting its CPU weight in relation to that of other virtual systems.

You must identify any anticipated burstiness while the security system is in fair mode, and then choose the CPU weight for each vsys appropriately so that bursts pass through the security system. We recommend verifying that adverse packet dropping does not occur with the chosen weights prior to deployment. With this feature, you can also ensure a fixed CPU weight for the root vsys.

For more information on setting and viewing CPU limits, see *Concepts & Examples ScreenOS Reference Guide*.

**Related  
Documentation**

- [Vsys DHCP Enhancement Overview on page 353](#)
- [Vsys Limitations Overview on page 354](#)
- [Vsys Clusters Overview on page 376](#)
- [Vsys Session Limit Overview on page 356](#)
- [Example: Configuring Vsys Resource Limits \(NSM Procedure\) on page 355](#)

---

## Example: Configuring CPU Limit (NSM Procedure)

---

To configure Vsys CPU limit:

1. In the NSM navigation tree, select **Object Manager > Vsys Profile**.
2. Select an existing vsys profile object and click **Edit**.
3. For CPU Weight, enter **40**.
4. Click **OK** to apply the setting.

**Related  
Documentation**

- [Policy-Based Routing Overview on page 349](#)
- [Vsys DHCP Enhancement Overview on page 353](#)
- [Vsys Limitations Overview on page 354](#)
- [Vsys Session Limit Overview on page 356](#)
- [Example: Configuring Vsys Session Limit \(NSM Procedure\) on page 356](#)

## CHAPTER 12

# User Authentication

This chapter explains the options available for using Extensible Authentication Protocol (EAP) to provide authentication for Ethernet and wireless interfaces. It contains the following topics:

- [IEEE 802.1x Support Overview on page 359](#)
- [Supported EAP Types on page 360](#)

### IEEE 802.1x Support Overview

---

EAP is an authentication framework that supports multiple authentication methods. EAP typically runs directly over data link layers, such as Point-to-Point Protocol (PPP) or IEEE 802, without requiring Layer 3 addressing.

IEEE 802.1X works for port-based access control, and IKEv2 uses it as an option for authentication. EAP functions in a security device configured in Transparent or Route (with or without Network Address Translation enabled) mode. Network and Security Manager (NSM) NetScreen Redundancy Protocol (NSRP) supports EAP in networks with high availability. Log messages and SNMP support are also available.

IEEE 802.1X support is available for all platforms.

EAP functions as the authentication portion of PPP, which operates at Layer 2. EAP authenticates a supplicant, or client, after the supplicant sends proper credentials and the authentication server, usually a RADIUS server, defines the user-level permissions. When you use EAP, all authentication information passes through the security device (known as a pass-through method of EAP authentication). All user information is stored on the authentication server.

If you use a RADIUS server for authentication that supports vendor-specific attributes (VSAs), you can use the zone-verification feature to verify the zones in which a client is a member.

#### Related Documentation

- [Route Types Overview on page 293](#)
- [Routing Table Entries Overview on page 303](#)
- [RIP Overview on page 319](#)
- [Supported EAP Types on page 360](#)

- [Creating an NSRP Cluster on page 363](#)
- [Configuring Active/Passive Cluster on page 364](#)
- [Example: Configuring Active/Passive Cluster \(NSM Procedure\) on page 365](#)

## Supported EAP Types

The supported EAP types are displayed in [Table 88 on page 360](#).

**Table 88: Supported EAP Types**

Parameters	Description
EAP-TLS (Transport Layer Security)	EAP-TLS is the most common EAP derivative and is supported by most RADIUS servers. EAP-TLS uses certificates for user and server authentication and for dynamic session key generation.
EAP-TTLS (Tunneled Transport Layer Security)	EAP-TTLS requires only a server-side certificate and a valid username and password for authentication. Steel-Belted RADIUS supports TTLS.
EAP-PEAP (Protected EAP)	EAP-PEAP compensates for the lack of features in EAP-TLS and reduces management complexity. It requires only server-side certificates and a valid username and password. It provides support for key exchange, session resumption, fragmentation, and reassembly. Steel-Belted RADIUS and Microsoft IAS support Protected EAP.
EAP-MD5 (Message Digest Algorithm 5)	Algorithm that uses a challenge and response process to verify MD5 hashes.

### Related Documentation

- [Route Types Overview on page 293](#)
- [Routing Table Entries Overview on page 303](#)
- [RIP Overview on page 319](#)
- [IEEE 802.1x Support Overview on page 359](#)
- [Creating an NSRP Cluster on page 363](#)
- [Configuring Active/Passive Cluster on page 364](#)
- [Example: Configuring Active/Passive Cluster \(NSM Procedure\) on page 365](#)

## CHAPTER 13

# High Availability

High availability (HA) provides a way to minimize the potential for device failure within a network. Because all of your network traffic passes through a Juniper Networks security device, you need to remove as many points of failure as possible from your network by ensuring that the device has a backup in case it fails.

Setting up your security devices in HA pairs removes one potential point of failure from your network design. You can remove other potential points of failure by setting up redundant switches on either side of the HA pair of security devices. This chapter explains how to configure NSM NetScreen Redundancy Protocol (NSRP) clusters and describes how to use NSRP to support HA.

For detailed information on NSRP and HA, see the *Concepts & Examples ScreenOS Reference Guide*.

This chapter contains the following topics:

- [NSRP Clusters Overview on page 361](#)
- [Creating an NSRP Cluster on page 363](#)
- [Configuring Active/Passive Cluster on page 364](#)
- [Example: Configuring Active/Passive Cluster \(NSM Procedure\) on page 365](#)
- [Active/Active Configurations Overview on page 368](#)
- [Configuring an Active/Active Cluster \(NSM Procedure\) on page 369](#)
- [Synchronizing Virtual Router Configurations and RunTime Objects \(NSM Procedure\) on page 369](#)
- [Changing VSD Group Member States \(NSM Procedure\) on page 371](#)
- [Example: Changing VSD Group Member States \(NSM Procedure\) on page 372](#)
- [Configuring NSRP to Detect Interface and Zone Failure on page 373](#)
- [Vsys Clusters Overview on page 376](#)
- [Exporting and Importing Device Configurations \(NSM Procedure\) on page 377](#)

## NSRP Clusters Overview

---

An NSRP cluster consists of two security devices that enforce the same security policy and share the same configuration settings. When you assign a security device to an NSRP

cluster, any changes you make to the configuration on one member of the cluster propagate to the other. Members of the same NSRP cluster maintain identical settings for policies and policy objects (such as addresses, services, VPNs, users, and schedules) and system parameters (such as settings for authentication servers, DNS, SNMP, syslog, and so on).

Before two security devices can provide redundant network connectivity, you must group them in the same NSRP cluster. In an NSRP cluster, one device acts as a primary and the other as a backup:

- In active/passive configurations, the primary device handles all firewall and VPN activities while the backup waits to take over when the primary fails. You can configure the cluster in active/passive operation when the interfaces are in Transparent, NAT, or Route mode:
  - Transparent Mode. When interfaces are in Transparent mode, security zone interfaces do not have IP addresses, and the security device forwards traffic like a Layer 2 switch. To manage a backup device, you use the manage IP address that you set on the VLAN1 interface.
  - NAT or Route Mode. When interfaces are in NAT or Route mode, the security zone interfaces have IP addresses, and the device forwards traffic like a Layer 3 router. To manage a backup device, you must use the manage IP address that you set per security zone interface; you cannot set a manage IP address on a virtual security interface (VSI) for any virtual security device (VSD) group except VSD group 0.
- In active/active configurations, you create two VSD groups for the cluster: One device acts as the primary device of one VSD group, while the other device acts as the backup for the same group. In the other VSD group, the device roles are reversed: Each device is the primary device of one VSD group and the backup in the other VSD group. You can configure the cluster in active/active operation when the interfaces are in NAT or route mode. The security zone interfaces have IP addresses, and the device forwards traffic like a Layer 3 router. To manage a backup device, you must use the manage IP address that you set per security zone interface; you cannot set a manage IP address on a VSI for any VSD group except VSD group 0.

Because of the sensitive nature of NSRP communications, you can secure all NSRP traffic through encryption and authentication. For encryption and authentication, NSRP supports the DES and MD5 algorithms respectively. However, if the HA cables run directly from one security device to another (that is, not through a switch forwarding other kinds of network traffic), it is unnecessary to use encryption and authentication.

In addition to NSRP clusters, which propagate configurations among group members and advertise each members' current VSD group states, you can configure the devices as members in a runtime object (RTO) mirror group, which maintains the synchronicity of RTOs between a pair of devices. When the primary device fails, the backup becomes the primary device with minimal service downtime by maintaining all current sessions.



**NOTE:** We recommend that you do not change the settings of VSD group 0 after importing the NSRP to NSM. Doing so will result in a loss of most attributes, especially the interface attributes. If you must change VSD group 0 settings, do not use NSM to delete or add VSD group 0. The safe way is to use the CLI or the Web UI to make the change to the device cluster first, and then reimport the cluster to NSM. On devices running ScreenOS 6.3, NSRP supports IPv6.

For more information about NSRP, see the *Concepts & Examples ScreenOS Reference Guide: NSRP* for ScreenOS 5.x or the *Concepts & Examples ScreenOS Reference Guide: High Availability*.

#### Related Documentation

- [Route Types Overview on page 293](#)
- [Routing Table Entries Overview on page 303](#)
- [RIP Overview on page 319](#)
- [IEEE 802.1x Support Overview on page 359](#)
- [Supported EAP Types on page 360](#)
- [Creating an NSRP Cluster on page 363](#)
- [Configuring Active/Passive Cluster on page 364](#)
- [Example: Configuring Active/Passive Cluster \(NSM Procedure\) on page 365](#)

## Creating an NSRP Cluster

To create an NSRP cluster:

1. In the NSM navigation tree, select **Device Manager > Devices**. Double-click the device object to open the device configuration.
2. Click the **Add** icon and select **Cluster**.
3. Follow the directions in the Add Device wizard to add the cluster.



**NOTE:** When you select the device model and ScreenOS version, remember that all devices in a cluster must be the same device model and run the same ScreenOS version.

4. Right-click the cluster and select **New > Cluster Member**.
5. Follow the directions in the Add Device wizard to import or model the cluster member.



**NOTE:** When importing cluster device members, ensure that their device configurations are in sync (errors can occur in the import process if you attempt to import out-of-sync configurations).

Finally, configure the cluster and the cluster members (you must configure cluster members from within the cluster itself). To configure a cluster member:

1. In the NSM navigation tree, select **Device Manager > Cluster**. Double-click the cluster object to open the cluster configuration.
2. Select **Members in the Cluster**.
3. Double-click the cluster member you want to configure to open its device configuration, then make your changes.

Most settings entered on one device in a cluster propagate to the other device, however, some configurations, such as setting NSRP authentication and encryption passwords, do not propagate. If you are using NSRP authentication and encryption passwords in the cluster, you need to configure the same information on all devices in the cluster.

For instructions for adding member devices to a cluster, see the *Network and Security Manager Online Help* topic "Configuring NSRP Clusters."

For more information about configurations that do not propagate, see the *Concepts & Examples ScreenOS Reference Guide: NSRP* for ScreenOS 5.x or *Concepts & Examples ScreenOS Reference Guide: High Availability*.

#### Related Documentation

- [Route Types Overview on page 293](#)
- [Routing Table Entries Overview on page 303](#)
- [RIP Overview on page 319](#)
- [IEEE 802.1x Support Overview on page 359](#)
- [Supported EAP Types on page 360](#)
- [NSRP Clusters Overview on page 361](#)
- [Configuring Active/Passive Cluster on page 364](#)
- [Example: Configuring Active/Passive Cluster \(NSM Procedure\) on page 365](#)

---

## Configuring Active/Passive Cluster

In an active/passive configuration, the primary device propagates all its network and configuration settings and the current session information to the backup device. If the primary device fails, the backup device becomes the primary device and takes over the traffic processing.



**NOTE:** When using a PPPoE connection to an ISP for Internet access, you can bind the PPPoE instance to a VSI interface. In the event of failover, this configuration enables the new master to use the same IP and PPPoE connection as the previous master. For details, see "[About Configuring PPPoE](#)" on page 135.

---



By default, the two cluster members are configured as active/passive after you add them to the cluster object. NSM automatically creates VSD group 0 and transforms physical interfaces into virtual security interfaces (VSIs) for VSD group 0.

To configure an active/passive cluster, you must:

1. Cable two security devices together.
2. Select automatic **RTO synchronization**.
3. Select the ports that you want the devices to monitor, so that if they detect a loss of network connectivity from one of the monitored ports, the primary device fails over.

#### Related Documentation

- [Route Types Overview on page 293](#)
- [Routing Table Entries Overview on page 303](#)
- [RIP Overview on page 319](#)
- [IEEE 802.1x Support Overview on page 359](#)
- [Supported EAP Types on page 360](#)
- [NSRP Clusters Overview on page 361](#)
- [Creating an NSRP Cluster on page 363](#)
- [Example: Configuring Active/Passive Cluster \(NSM Procedure\) on page 365](#)

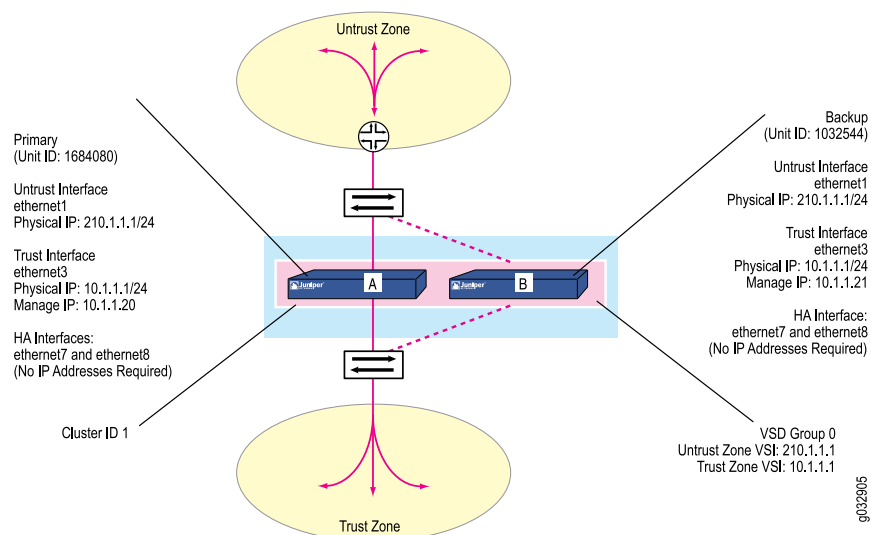
### Example: Configuring Active/Passive Cluster (NSM Procedure)

In this example, you configure two NetScreen-208 security devices, Corporate A and Corporate B, in an NSRP cluster. Both devices are running ScreenOS 5.x. Using a cable, connect the ethernet7 interfaces of both devices, and then use another cable to connect the ethernet8 interfaces. Next, add the cluster and cluster member to NSM. When the devices become members of the NSRP cluster, the IP addresses of their physical interfaces automatically become the IP addresses of the virtual security interfaces (VSIs) for VSD group ID 0. Each VSD member has a default priority of 100. The device with the higher unit ID becomes the VSD group primary. See [Figure 6 on page 366](#).

Finally, configure the cluster:

- Bind ethernet7 and ethernet8 to the HA zone. By default, ethernet8 is bound to the HA zone, so you only need to bind it to the HA zone if you have previously bound it to a different zone.
- Set manage IP addresses for the Trust zone interfaces on both devices.
- Configure monitoring on ethernet1 and ethernet3 so that loss of network connectivity on either of those ports triggers a device failover.
- Select automatic synchronization of RTOs.

Figure 6: Example of NSRP Active/Passive Configuration



To configure an active/passive cluster:

- In the NSM navigation tree, select **Device Manager > Devices**. Click the Add icon and select **Cluster**. The Cluster screen is displayed. Configure the following, then click **OK**:
  - For Cluster Name, enter **Corporate**.
  - For Color, select **cyan**.
  - For Physical Choice, select **ns208**.
  - For OS Version, select **5.0**.
  - Ensure that Transparent Mode is not enabled (unchecked).
  - For License Model, select **Advanced**.
- Add the following two cluster members to the cluster: Corporate A, Corporate B. Choose **Model** when adding each device.
- Configure the HA interfaces for the cluster.
- In the cluster navigation tree, select **Network > Interface**. Double-click **ethernet7**. The General Properties screen appears.
- For Zone, select **HA**, and then click **OK** to save your changes.
- Double-click **ethernet8**. The General Properties screen appears.
- Ensure that the zone name is HA, and then click **OK** to save your changes.
- Configure the Untrust interface for the cluster:
  - In the cluster navigation tree, select **Network > Interface**. Double-click **ethernet1**. The General Properties screen appears.
  - For Zone, select **Untrust**.

- For IP address and netmask, enter **210.1.1.1/24**.
  - Click **OK** to save your changes.
9. Configure the Trust interface for the cluster:
    - In the cluster navigation tree, select **Network > Interface**. Double-click **ethernet3**. The General Properties screen appears.
    - For Zone, select **Trust**.
    - For IP address and netmask, enter **10.1.1.1/24**.
    - Ensure that the interface mode is NAT, and then click **OK** to save your changes.
  10. Click **Apply** to apply all previous changes to the cluster members.
  11. Configure the Manage IP and Monitoring for Corporate A:
    - In the cluster navigation tree, select **Members**. Double-click **Corporate A** to open its device configuration.
    - In the device navigation tree, select **Network > Interface** and double-click **ethernet 3**. The General Properties screen appears.
    - For Manage IP, enter **10.1.1.20**, and then click **OK** to save your changes.
  12. In the device navigation tree, select **Monitoring > Whole Box Monitoring**, and then select the **Monitor Interface** tab.
  13. Click the Add icon to display the new monitor interface dialog box. Select **ethernet1**, leave the default weight of 255, and click **OK** to save your changes.
  14. Click the Add icon to display the new monitor interface dialog box. Select **ethernet3**, leave the default weight of 255, and click **OK** to save your changes.
  15. Click **OK** to close the device configuration for Corporate A.
  16. Configure the Manage IP for Corporate B:
    - In the cluster navigation tree, select **Members**. Double-click Corporate B to open its device configuration.
    - In the device navigation tree, select **Network > Interface** and double-click **ethernet 3**. The General Properties screen appears.
    - For Manage IP, enter **10.1.1.21**, and then click **OK** to save your changes.
    - In the device navigation tree, select **Monitoring > Whole Box Monitoring**, and then select the **Monitor Interface** tab.
    - Click the Add icon to display the new monitor interface dialog box. Select **ethernet1**, leave the default weight of 255, and click **OK** to save your changes.
    - Click the Add icon to display the new monitor interface dialog box. Select **ethernet3**, leave the default weight of 255, and click **OK** to save your changes.
    - Click **OK** to close the device configuration for Corporate B.
  17. Configure the NSRP settings:
    - In the cluster navigation tree, select **NSRP**.

- Select **RTO Sync**.

18. Click **OK** to save your changes to the cluster and cluster members.

**Related  
Documentation**

- [Route Types Overview on page 293](#)
- [Routing Table Entries Overview on page 303](#)
- [RIP Overview on page 319](#)
- [NSRP Clusters Overview on page 361](#)
- [Active/Active Configurations Overview on page 368](#)
- [Creating an NSRP Cluster on page 363](#)
- [Configuring Active/Passive Cluster on page 364](#)

---

## Active/Active Configurations Overview

---

On a security device in Route or NAT mode, you can configure both devices in a redundant cluster to be active, sharing the traffic distributed between them by routers with load-balancing capabilities running a protocol such as the Virtual Router Redundancy Protocol (VRRP).

Using NSRP, you create two virtual security device (VSD) groups, each with its own virtual security interfaces (VSIs). For example, Device A acts as the primary of VSD group 1 and as the backup of VSD group 2. Device B acts as the primary of VSD group 2 and as the backup of VSD group 1. Devices A and B each receive 50% of the network and VPN traffic. Should device A fail, device B becomes the primary of VSD group 1, as well as continuing to be the primary of VSD group 2, and handles all of the traffic.

In ScreenOS 6.1 or later, on a security device in Transparent mode, the Active/Active mode provides system monitoring and traffic load-sharing by using VLANs to differentiate traffic to different VSDs. NSM allows the user to assign or unassign a VLAN group to a VSD. The user needs to set the VSD group in cluster mode and the VSD group ID list is available from the cluster member. All VLANs belonging to the group are assigned to the VSD group. The user can assign multiple VLAN groups to a VSD group as well.

Although the total number of sessions divided between the two devices in an active/active configuration cannot exceed the capacity of a single security device (otherwise, in the case of a failover, the excess sessions might be lost), the addition of a second device doubles the available bandwidth potential. A second active device also guarantees that both devices have functioning network connections.

**Related  
Documentation**

- [Route Types Overview on page 293](#)
- [Routing Table Entries Overview on page 303](#)
- [RIP Overview on page 319](#)
- [NSRP Clusters Overview on page 361](#)
- [Creating an NSRP Cluster on page 363](#)

- [Configuring Active/Passive Cluster on page 364](#)

## Configuring an Active/Active Cluster (NSM Procedure)

To configure an active/active cluster, you must configure a second VSD group:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Double-click the cluster to open the cluster configuration. In the cluster navigation tree, select **Members**.
3. In the VSD definitions area, click the Add icon to display the Add VSD dialog box.
4. Select a value, and then click **OK** to save the new VSD. The VSD you added appears in the VSD Definitions list.
5. Select **Network > Vlan > Group**, and click the Add icon to display the New Vlan Group Entry dialog box.
6. Enter the VLAN group name, VLAN group settings, binding VLAN group to port and zone settings, and select any value in the VSD group ID. The value of the VSD group ID is the list of VSD definitions from the NSRP members.
7. Click **OK** to save your changes to the cluster.

The VSD group member with the priority number closest to 0 becomes the primary. (The default is 100.) If two devices have the same priority value, the device with the lowest MAC address becomes primary.

### Related Documentation

- [Virtual Routers Overview on page 294](#)
- [Virtual Router General Properties Overview on page 295](#)
- [NSRP Clusters Overview on page 361](#)
- [Creating an NSRP Cluster on page 363](#)
- [Active/Active Configurations Overview on page 368](#)
- [Configuring Active/Passive Cluster on page 364](#)
- [Synchronizing Virtual Router Configurations and RunTime Objects \(NSM Procedure\) on page 369](#)

## Synchronizing Virtual Router Configurations and RunTime Objects (NSM Procedure)

The virtual router synchronization tasks are as follows:

- [Synchronizing Virtual Router Configurations on page 370](#)
- [Configuring the Virtual Router Synchronization Settings on page 370](#)
- [Synchronizing Runtime Objects on page 371](#)

## Synchronizing Virtual Router Configurations

After you add new members to an NSRP cluster, you must synchronize the configuration and files from one device to another.

To synchronize configurations:

1. In the NSM navigation tree, select **Device Manager > Devices**, and then double-click the cluster to open the cluster configuration.
2. In the Device Manager, double-click the cluster to open the cluster configuration.
3. In the cluster navigation tree, select **NSRP Directives > Flash Sync**.
4. Select the device that will be used to synchronize the other device and click **Perform Sync**. The device that has been synchronized is automatically rebooted to activate the new configuration.
5. Click **OK** to save your changes to the cluster.

## Configuring the Virtual Router Synchronization Settings

You can configure the virtual router information for the cluster or cluster members. For devices running 5.0, you must configure the virtual router settings at the system level (the cluster).

For devices running ScreenOS 5.1 and later, you can configure the virtual router setting at the system level (the cluster) or at the local level (cluster member). By default, cluster members automatically use the virtual router settings of the cluster. To use different router settings for each cluster member, you must disable NSRP configuration synchronization for the router at the system level:

1. In the NSM navigation tree, select **Device Manager > Devices**, and then double-click the cluster to open the cluster configuration.
2. In the cluster navigation tree, select **Network > Virtual Router**. Double-click the trust-vr virtual router. The General Properties screen appears.
3. Clear the **Enable NSRP Configuration Sync for Vrouter** check box, and then click **Apply** to save your changes to the cluster.
4. In the cluster navigation tree, select **Members** and double-click a cluster member device to open the device configuration. Edit the virtual router settings as desired.



**NOTE:** The Enable NSRP Configuration Sync setting does not affect the virtual router ID. The virtual router ID setting is always configured at the local level (cluster member).

---

5. Click **OK** to save your changes to the cluster member, and then click **OK** to save your changes to the cluster.

## Synchronizing Runtime Objects

After synchronizing the configurations and files, you can then synchronize the runtime objects (RTOs). RTOs are code objects created dynamically in memory during normal operation. Some examples of RTOs are session table entries, ARP cache entries, DHCP leases, and IPsec security associations (SAs). In the event of a failover, the new primary device must maintain the current RTOs to avoid service interruption.

To ensure session back up, the members of an NSRP cluster backup the RTOs using an RTP mirror group. An RTO mirror group is two security devices that pass RTOs unidirectionally from a sender to a receiver. You can also create a second mirror group (with a different group ID from the first group) for the same devices but reverse the roles of sender and receiver. Working together, each member backs up the RTOs from the other, which permits RTOs to be maintained if the primary device of either VSD group in an active/active HA scheme fails.

After you add the cluster members, you can configure RTO synchronization to enable each member to send and receive RTOs. However, by default, NSRP cluster members do not synchronize their configurations before synchronizing RTOs; before enabling RTO synchronization, you must first synchronize the configurations between the cluster members. Unless the configurations on both members in the cluster are identical, RTO synchronization might fail.

### Related Documentation

- [Virtual Routers Overview on page 294](#)
- [Virtual Router General Properties Overview on page 295](#)
- [NSRP Clusters Overview on page 361](#)
- [Creating an NSRP Cluster on page 363](#)
- [Active/Active Configurations Overview on page 368](#)
- [Configuring an Active/Active Cluster \(NSM Procedure\) on page 369](#)
- [Configuring Active/Passive Cluster on page 364](#)
- [Changing VSD Group Member States \(NSM Procedure\) on page 371](#)

## Changing VSD Group Member States (NSM Procedure)

If necessary, for troubleshooting or maintenance, you can force a device to assume a new mode (master, backup, or ineligible) in a specified VSD group. To change a VSD group member state:

1. In the NSM navigation tree, select **Device Manager > Devices**, and then double-click the cluster to open the cluster configuration.
2. In the Device Manager, double-click the cluster to open the cluster configuration.
3. In the cluster navigation tree, select **NSRP Directives > Exec Mode**.
4. Select the device that will assume a new role, and then click **Exec Mode**. The Mode Selection dialog box appears.

5. Select the mode that the device is to assume:
  - Master—The VSD group member (primary device) that processes traffic sent to the VSI.
  - Backup—The VSD group member that becomes the primary device if the current primary device fails. The election process uses device priorities to determine which member to promote. When electing a new primary, an RTO peer has precedence over any other VSD group member, even if that member has a better priority rating.
  - Ineligible—The VSD group member that cannot participate in the election process. The preempt option must be enabled on the master device for this option to appear.
6. Click **OK** to save your changes.

**Related  
Documentation**

- [NSRP Clusters Overview on page 361](#)
- [Creating an NSRP Cluster on page 363](#)
- [Active/Active Configurations Overview on page 368](#)
- [Example: Changing VSD Group Member States \(NSM Procedure\) on page 372](#)

---

### Example: Changing VSD Group Member States (NSM Procedure)

---

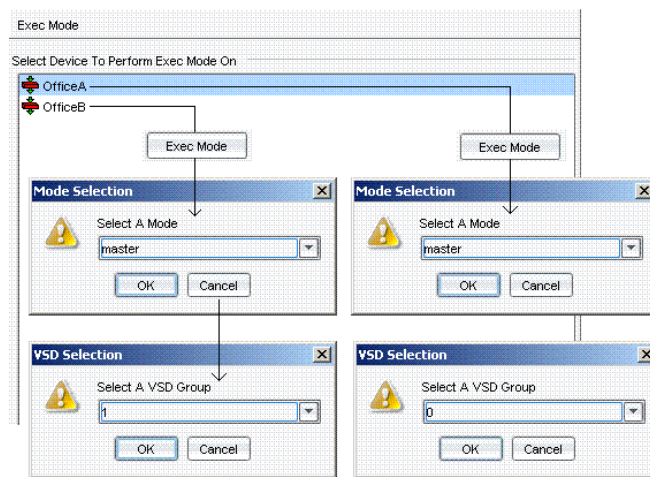
To change the VSD group member state:

1. In the NSM navigation tree, select **Device Manager > Devices**, and then double-click the cluster to open the cluster configuration.
2. In the cluster navigation tree, select **NSRP Directives > Exec Mode**.
3. Select **Office A**, and then click **Exec Mode**. Configure as master (primary) of VSD group 0.
4. Select **Office B**, and then click **Exec Mode**. Configure as master (primary) of VSD group 1.

Both configurations are shown in [Figure 7 on page 373](#).



Figure 7: Configuring VSD Group Masters



5. Click **OK** to save your changes to the cluster.

#### Related Documentation

- [NSRP Clusters Overview on page 361](#)
- [Creating an NSRP Cluster on page 363](#)
- [Active/Active Configurations Overview on page 368](#)
- [Changing VSD Group Member States \(NSM Procedure\) on page 371](#)
- [Configuring NSRP to Detect Interface and Zone Failure on page 373](#)

## Configuring NSRP to Detect Interface and Zone Failure

You can configure NSRP to detect interface and zone failures on a device or VSD group. When one or more monitored objects on a device or VSD group fail, the primary device in the cluster or VSD group can fail over to the backup device or VSD group.

To control when the device or VSD group fails over, you configure the device to monitor specific objects.



**NOTE:** Each vsys cluster device can see all VSDs in the cluster, even VSDs that the Vsys cluster device does not use. This means that you could configure a vsys cluster device to monitor a VSD group that the device does not use. If this monitored VSD group failed, the vsys cluster device that does use that VSD group would failover—not the vsys cluster device that was configured to monitor the VSD group.

For each device or VSD group, you can monitor:

- Specific target IP addresses—The device sends ping or ARP requests to up to 16 specified IP addresses at specified intervals and then monitors responses from the targets. All the IP addresses configured on the device or for a specified VSD group constitute a single monitored object.
- Physical interfaces—The device uses NSRP to check that the physical ports are active and connected to other devices.
- Zones—The device uses NSRP to check that all physical ports in a zone are active.

For each monitored object, you must configure a threshold, which is the total weight of failed monitored objects required to cause the device or VSD group to step down as master. If the cumulative weight of the failures of all monitored objects exceeds the monitored object failure threshold and the monitor threshold, then the device or VSD group fails over to the backup device or VSD group. You can set the monitored object failover threshold to a value from 1 to 255. The default threshold is 255.

You must also configure a failure weight, which is the weight that the failure of the monitored object contributes towards the device or VSD group failover threshold, which is known as the monitor threshold. You can set the object failure weight at a value from 1 to 255. The default failure weight for monitored objects is 255. If you want to monitor an object but do not want the failure of the object to affect failover of the device or VSD group, set the failure weight of the object to 0 (all failures are logged, even if the failure weight of the object is 0).

## Configuring Track IPs

For tracked IP addresses, you specify individual IP addresses, how they are to be monitored, what constitutes the failure of each tracked IP address (the threshold), and the weight that each failed address carries. When IP tracking is enabled, the device sends a request on the selected interface to target IP addresses at specified intervals, and then monitors the targets for responses. If the device does not receive a response from a target for a specified number of times, the device considers that IP address to be unreachable. You configure the threshold (the number of acceptable consecutive response failures) for each IP address within the IP Option dialog box. The default threshold for each IP address is 3; acceptable values are from 1 to 200.

If the device does not receive a response from a specified number of targets, the device can deactivate routes associated with the selected interface. This threshold, known as the failure threshold, is the sum of the weights of all failed tracked IP addresses required for the tracked IP object to be considered failed. You configure the interface threshold

(the total weight of the cumulative failed attempts) in the Track IP tab. The default is 1; acceptable values are from 1 to 255. A failure to reach any configured tracked IP address causes routes associated with the interface to be deactivated.

For each interface, you can configure up to four IP addresses to track. The tracked IP addresses do not have to be in the same subnet as the interface. On devices running ScreenOS 6.3, track IPs supports IPv6.



**NOTE:** A single device can track 64 IP addresses. This total includes all track IP addresses for interface-based IP tracking and for NSRP-based IP tracking at the root level and vsys level.

## Configuring Interface Monitoring

The device uses NSRP to check that the physical ports are active and connected to other network devices. When the port is inactive, the device considers the interface failed.

The process for adding an interface to monitor is as follows:

- Edit the cluster by selecting and editing its members.
- Select **Monitoring > Whole Box Monitoring**.
- Use the Monitor Interface tab to select all the interfaces that need to be monitored and assign a weight to each interface in the device or VSD group to indicate the importance of that interface. The higher the weight, the faster the failover threshold is met. For example, if the untrust interface is more important than the management interface, assign the untrust interface a higher weight than the management interface.

For example, when using two VSD groups (VSD 1 and VSD 2) configured on two devices (device A and device B), if a port on a master device in a VSD group fails, you can configure VSD 1 to fail over from the primary VSD group on device A to the backup VSD group on device B. VSD 2 remains active on device A.

## Configuring Zone Monitoring

The device uses NSRP to check that all physical ports in a zone are active and connected to other network devices. When all ports within the zone are inactive, the device considers the zone failed.

You can assign a weight to each zone in the device or VSD group to indicate the importance of that zone. The higher the weight, the faster the failover threshold is met. For example, if the DMZ zone is more important than the trust zone, assign the DMZ zone a higher weight than the trust zone.

All interfaces bound to the monitored zone must fail before the device considers the zone down. Specifically:

- If a monitored zone has multiple interfaces, but only one interface in the zone is active, the device considers the zone active.
- If a monitored zone has a single interface bound to it and that interface fails, the device considers the zone failed.
- If a monitored zone has no interfaces bound to it, the zone cannot fail.
- If you unbind a downed interface from a zone that contains only that interface, the device no longer considers the zone failed. Similarly, if you unbind an active interface from a monitored zone where the remaining interfaces are down, the device considers the zone failed.

## Configuring Monitor Threshold

The monitor threshold is the failure threshold for the device or VSD group. All failure weights for all monitored objects in the device or VSD group contribute to the monitor threshold when a failure occurs; if the total sum of these failure weights meets or exceeds the monitor threshold, the device or VSD group fails over.

Alternatively, even if all IP addresses, interfaces, and the zone fail in the device or VSD group, if the sum of their failure weights does not meet or exceed the monitor threshold, the device or VSD group does not fail over to the backup VSD group. To ensure that the device or VSD group fails over at the appropriate time, configure the failure weights of each monitored object in relation to the monitor threshold.

### Related Documentation

- [NSRP Clusters Overview on page 361](#)
- [Creating an NSRP Cluster on page 363](#)
- [Active/Active Configurations Overview on page 368](#)
- [Changing VSD Group Member States \(NSM Procedure\) on page 371](#)

---

## Vsys Clusters Overview

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

To enable failover from one virtual system to another, you must create a virtual system interface (VSI) for each virtual system. A logical entity at Layer 3 is linked to multiple Layer 2 physical interfaces in a VSD group. The VSI binds to the physical interface of the device acting as primary 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 primary.

- Trust zone VSIs—Each vsys has its own trust zone VSI by default. All trust zone VSIs must be in different subnets.
- Untrust zone VSIs—You can configure each vsys to use its own untrust zone VSI or share the untrust zone VSI from the root device. When virtual systems have their own untrust zone VSIs, the VSIs must be in different subnets from each other and from the untrust zone VSI at the root level.

After creating VSI, you must also create VSD groups to contain these VSIs.

In ScreenOS 6.1 high-end platforms, NSM allows the user to assign or unassign a VLAN group to a VSD. The user can create VLAN groups only after importing the VVLANlan in the members. The user needs to set the VSD group in cluster mode and the VSD group ID list is available from the cluster member. All VLANs belonging to the group will be assigned to the VSD group. The user can assign multiple VLAN groups to a VSD group as well.

**Related  
Documentation**

- [NSRP Clusters Overview on page 361](#)
- [Creating an NSRP Cluster on page 363](#)
- [Active/Active Configurations Overview on page 368](#)
- [Changing VSD Group Member States \(NSM Procedure\) on page 371](#)

## Exporting and Importing Device Configurations (NSM Procedure)

Use the Export Device Config To File directive to export an existing configuration on a security device(s) to a file.

To export a device configuration to a file:

1. In the NSM navigation tree, select **Device Manager > Devices**, and select a security device.
2. From the Devices menu, select **Configuration > Export Device Config To File**.
3. Select a security device(s). Click **OK**. A Job Information window appears displaying the status of the export process.
4. Click the device(s) whose configuration(s) you want to save, and then click **Save Selected**.

After the export has completed, you can then use the Import Device Config From File function to import that configuration to a security device.

To import a device config from a file:

1. In the NSM navigation tree, select **Device Manager > Devices**, and select a security device.
2. From the Devices menu, select **Configuration > Import Device Config From File**. A Select Target Directory window appears.
3. Select the configuration file. Pay careful attention to select a configuration file that was exported from the same type of security device running the same version of ScreenOS.
4. Click **Import**. A Job Information window appears displaying the status of the import process.

**Related  
Documentation**

- [NSRP Clusters Overview on page 361](#)
- [Creating an NSRP Cluster on page 363](#)

- [Active/Active Configurations Overview on page 368](#)
- [Changing VSD Group Member States \(NSM Procedure\) on page 371](#)

## CHAPTER 14

# WAN, ADSL, Dial, and Wireless

Juniper Networks wireless devices and systems provide wireless local area network (WLAN) connections with integrated IP Security virtual private network (IPsec VPN) and firewall services for wireless clients, such as telecommuters, branch offices, or retail outlets.

This chapter contains the following topics:

- [Wireless Settings in a Security Device Overview on page 379](#)
- [Configuring General Wireless Settings on page 380](#)
- [Configuring Advanced Wireless Settings on page 383](#)
- [Configuring Wireless MAC Access Lists on page 387](#)
- [Configuring Wireless General SSID Settings on page 388](#)
- [Configuring SSID Authentication and Encryption on page 389](#)
- [Reactivating Wireless Connections on page 394](#)
- [Conducting a Site Survey for Detecting Access Points on page 395](#)
- [Network, Interface, and Security Modules Supported in Security Devices on page 395](#)
- [Chassis Information Overview on page 399](#)
- [WPA2, Extended Range, and Super G Support on NetScreen5GT Wireless Overview on page 399](#)
- [Wi-Fi Protected Access Overview on page 400](#)
- [Configuring Wi-Fi Protected Access \(NSM Procedure\) on page 400](#)
- [Super G Methods Overview on page 402](#)
- [Configuring Atheros XR \(NSM Procedure\) on page 402](#)

### Wireless Settings in a Security Device Overview

---

The wireless settings specify how a wireless-capable security device connects multiple wireless networks or a wireless network to a wired network. You can configure wireless settings only on a Juniper Networks NetScreen-5GT Wireless security device running ScreenOS 5.0.0-WLAN or ScreenOS 5.0.0-DSLW; these devices can act as a wireless access point (WAP).

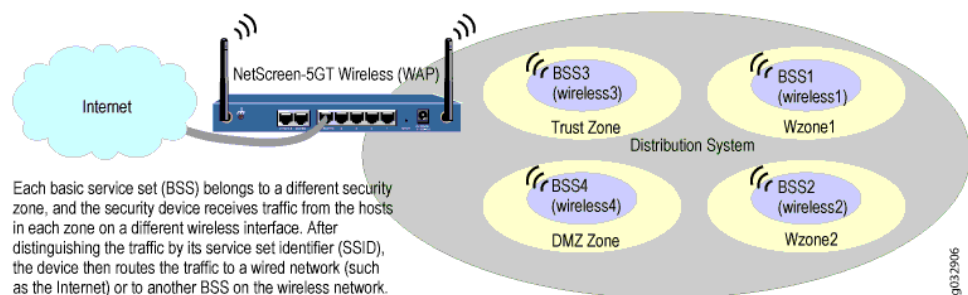
When you deploy a NetScreen-5GT Wireless as a WAP, the security device manages a distribution system of one to eight basic service sets (BSSs). Each BSS uses a unique name identifier, called a service set identifier (SSID). Each host within a BSS must have the same SSID as that configured for that BSS on the security device. When configuring the SSID, you bind each BSS to its own interface (and zone); segmenting BSSs enables you to enforce different levels of device authentication and encryption for each zone, and to create rules that control wireless traffic across zones.



**NOTE:** When security zones contain wireless and wired networks, they must use separate subnets and connect to the device through different interfaces with logically separate IP addresses.

The NetScreen-5GT Wireless security device supports up to 60 wireless clients concurrently.

**Figure 8: Using the NetScreen-5GT Wireless as a WAP**



#### Related Documentation

- [Virtual Routers Overview on page 294](#)
- [Configuring Advanced Wireless Settings on page 383](#)
- [Configuring Wireless MAC Access Lists on page 387](#)
- [Configuring Wireless General SSID Settings on page 388](#)
- [Configuring SSID Authentication and Encryption on page 389](#)

## Configuring General Wireless Settings

NetScreen-5GT Wireless security device contains a radio transmitter/receiver with a frequency range of 2.4 GHz to 2.4835 GHz, and supports the IEEE 802.11b and 802.11g standards. When you first deploy the NetScreen-5GT Wireless device on your network, the radio transmitter/receiver is configured with default settings designed to work in most networking environments.

You can edit the default values for the following radio settings:

- Antenna settings
- Channel settings



- Operation Mode settings
- Transmission Power and Rate settings

The following topics will detail each radio settings:

## Configuring Antennas

You can use one antenna or a pair of antennas on the NetScreen-5GT Wireless security device. Select the antenna option that meets your network needs and that corresponds to the actual physical antenna configuration on the device.

To configure the antenna, in the device navigation tree, select Wireless Settings then select one of the antenna configurations:

- Diversity antennas —Select this option when the security device is using a pair of diversity antennas that provide 2-dBi omnidirectional coverage (signal radiates 360 degrees horizontally). These antennas provide a fairly uniform level of signal strength within the area of coverage and are suitable for most installations (diversity antennas ship with the NetScreen-5GT Wireless device). This is the default option.
- Antenna A or Antenna B—Select one of these options when using a single antenna for 2-dBi omnidirectional coverage (signal radiates 360 degrees horizontally). Unlike diversity antennas, which function as a pair, the external antenna operates singly to eliminate an echo effect that can sometimes occur from slight delay characteristics in signal reception when two antennas are in use.



**NOTE:** On the NetScreen-5GT Wireless security device, antenna A is nearest the power connector port.

When importing wireless settings from a security device, Network and Security Manager (NSM) automatically displays the antenna settings configured on the physical device. Before activating a modeled wireless security device, however, you must ensure that the antenna setting you select in the NSM UI matches the actual antenna configuration on the physical device. For example, if you model the device using antenna A as a single antenna providing 2-dBi omnidirectional coverage, you or the device administrator must have connected an antenna to antenna port A on the physical device before you activate that device.

## Configuring Channels

The wireless security device uses channels to send and receive wireless traffic. The device uses the same channel for all basic service sets (BSSs), which share the same overall bandwidth, and distinguishes traffic from different BSSs by the SSID number.

By default, the wireless security device automatically selects the appropriate channel based on the country code. To select a specific channel, in the device navigation tree, select Wireless Settings and change the Channel for Wireless AP Radio setting to Channel Number, and then enter the channel number you want the device to use. To enable the device to use additional channels that might be available in your country, select **Extended Channel Mode**.

The regulatory domain for channel assignments is not configurable, and is preset as one of the following:

- FCC (USA)—This regulatory domain automatically sets the country code to USA. Because you cannot change this setting, it does not appear in the UI.
- TELEC (Japan)—This regulatory domain automatically sets the country code to Japan; you cannot change this setting. Because you cannot change this setting, it does not appear in the UI.
- WORLD (all countries)— This regulatory domain requires you to select from a list of countries (can select USA or Japan). If the device is preset to use FCC or TELEC, this setting does not appear in the UI.



**NOTE:** Although you can select the Extended Channel Mode option when the regulatory domain is WORLD and the selected country code is USA, there are no extended channels in the USA.

---

## Configuring Operation Mode Settings

The NetScreen-5GT Wireless supports both 802.11b and 802.11g operation modes, either simultaneously (default setting) or exclusively. To configure the operation mode, in the device navigation tree, select Wireless Settings and then select one of the following modes:

- To enable both 802.11b and 802.11g wireless clients to connect to the wireless security device, select **802.11b/g**.
- To enable only 802.11b wireless clients to connect to the wireless security device, select **802.11b**.
- To enable only 802.11g wireless clients to connect to the wireless security device, select **802.11b/g**, then select the **802.11g Only** check box.



**NOTE:** We recommend you enable CTS protection (see Configuring Control Frame Protection section in [“Configuring Advanced Wireless Settings” on page 383](#)) to avoid collisions when supporting 802.11b and 802.11g operation modes.

---

## Configuring Transmission Settings

Use the transmission settings to control the power and rate used by the wireless interfaces. To configure the transmission settings, in the device navigation tree, select **Wireless Settings**, and then edit the default values for the following settings:

- Transmit Power—This setting controls the power transmission and radio range. By default, the power level is set to full; available settings include an eighth, half, minimum, or quarter. You might need to edit this setting when using more than one wireless interface in the same location and frequency.

- Data Rate for AP—This setting controls the wireless interface data transmission rate for sending frames. By default, the rate is set to best rate (the wireless interface uses the best rate first, and then automatically falls back to the next rate if transmission fails).
- For 11b transmissions, available rates are 1, 2, 5.5, and 11mbps.
- For 11g transmissions, available rates are 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps.

**Related  
Documentation**

- [Virtual Routers Overview on page 294](#)
- [Wireless Settings in a Security Device Overview on page 379](#)
- [Configuring Advanced Wireless Settings on page 383](#)
- [Configuring Wireless MAC Access Lists on page 387](#)
- [Configuring Wireless General SSID Settings on page 388](#)
- [Configuring SSID Authentication and Encryption on page 389](#)

---

## Configuring Advanced Wireless Settings

Use the advanced wireless settings to control low-level wireless networking settings, such as aging values and collision protection. When you first deploy the NetScreen-5GT Wireless device on your network, the network settings are already configured with default settings designed to work in most networking environments. However, you might want to edit these settings to meet your specific wireless networking needs.

You can edit the default values for the following wireless networking settings.

- aging
- beacons
- burst and fragment size
- control frame protection
- short slots
- preambles

### Configuring Aging

The aging interval is the amount of time (in seconds) that a wireless client or bridge remembers an access point after communication with the WAP is lost. To configure the aging setting:

1. In the NSM navigation tree, select **Device Manager > Devices**. Double-click the device object to open the device configuration.
2. In the device navigation tree, select **Wireless Settings > Advanced**, and then edit the default aging value.

The default is 300 seconds; acceptable range is 60 to 1,000,000 seconds. To disable aging, set the value to 0 (zero).

## Configuring Beacons

A WAP broadcasts beacon packets to keep the wireless network synchronized and to inform wireless clients of waiting data. A beacon packet includes data such as the wireless LAN service area, the WAP address, and delivery traffic indicator maps (DTIMs).

To configure the beacon settings:

1. In the NSM navigation tree, select **Device Manager > Devices**. Double-click the device object to open the device configuration.
2. In the device navigation tree, select **Wireless Settings > Advanced**, and then edit the default values for the following settings:
  - **Beacon Interval**—The beacon interval is the amount of time between beacons sent by the NetScreen-5GT Wireless to wireless clients. A beacon transmission includes the beacon interval; the interval informs receiving devices how long they can wait in low-power mode before waking up to handle beacons. Increasing the beacon interval lessens the number of beacon responses required by a wireless client, enabling clients to reduce battery power. The default value is 100 time units; acceptable range is 20 to 1,000 time units (1 time unit equals 1024  $\mu$ s).
  - **Beacon Interval Between DTIMs**—This interval is the amount of beacon intervals between DTIM messages, which inform wireless clients of waiting data. A lower value enables wireless clients to download waiting data more often; a higher value enables wireless clients to wait in low-power mode longer between DTIMs. When using a high DTIM value, however, the client must stay active longer to collect waiting data, and clients might miss broadcast and multicast traffic messages. The default value is 1 beacon interval; acceptable range is 1 to 255.

## Configuring Burst and Fragment Size

Use the burst and fragment setting to configure how the device transmits wireless packets over the network. To configure the burst and fragment settings:

1. In the NSM navigation tree, select **Device Manager > Devices**. Double-click the device object to open the device configuration.
2. In the device navigation tree, select **Wireless Settings > Advanced**, and then edit the default values for the following settings:
  - **Maximum Number of Frames in a Burst**—The burst threshold defines the average maximum number of frames a WAP can use to handle wireless traffic before the device begins sending traffic in bursts. When wireless traffic exceeds the specified threshold, the device sends wireless packets in bursts to clients, who can switch to a low-power sleep state between bursts. The default value is 3 frames; acceptable range is 2 to 255 frames.
  - **Fragmentation Threshold**—The fragmentation threshold defines the maximum size of a packet that can be transmitted without fragmentation. If the packet size exceeds

the specified threshold, the sender (client or WAP) must fragment the packet before transmitting.

Using a high fragmentation threshold reduces the number of fragments on the wireless network, which can increase efficiency. However, large, unfragmented packets can be corrupted during transmission, requiring resend attempts that can decrease efficiency. The default value is 2346; acceptable range is even numbers between 256 and 2346.

## Configuring Control Frame Protection

Control frame protection is designed to help avoid collisions on the wireless network. Transmission collision usually occurs when two wireless devices are within range of the same WAP, but are not within range of each other (they are hidden nodes). If two wireless transmissions collide at the WAP, the data in each transmission is lost.

To avoid collisions, you can require wireless clients to first request permission to send data (clients must send a request-to-send (RTS) frame) and/or receive approval of that request (client must receive a clear-to-send (CTS) frame) before transmitting data.

Because 802.11b stations cannot hear 802.11g stations using orthogonal frequency-division multiplexing (OFDM), a method for wireless transmission that divides a signal and transmits the pieces at different frequencies simultaneously, traffic from these stations can collide on the network, reducing network efficiency. We recommend you enable protection to avoid collisions when supporting 802.11b and 802.11g operation modes.



**NOTE:** CTS protection is not supported when using 802.11b only.

To configure the control frame protection settings:

1. In the NSM navigation tree, select **Device Manager > Devices**. Double-click the device object to open the device configuration.
2. In the device navigation tree, select **Wireless Settings > Advanced**, and then edit the default values for the following settings:
  - **Threshold for RTS to Transmit**—The request-to-send (RTS) threshold defines the maximum size of a packet that a wireless client can send without obtaining permission from the WAP. If a packet exceeds this threshold, the client must send an RTS message to the WAP requesting permission to send the packet. You might want to adjust this setting to control traffic flow through an access point that services a large number of clients. The default is 2346; accepted range is 256 to 2346.
  - **CTS Protection Mode**—Enables clear-to-send (CTS) control frame protection, which requires wireless client to first receive a CTS frame from the WAP before sending data. Select one of the following protection modes:
    - **On**—When selected, wireless clients must first receive a CTS frame from the device before sending data.
    - **Off**—When selected, wireless clients do not send CTS control frames.

- Auto—When selected, the device automatically detects the CTS mode used by the wireless client. This is the default setting.
- CTS Protection Type—The protection type defines the level of control frame protection enforced by the device. Select one of the following protection types:
  - CTS Only—When selected, wireless clients must first receive a single, self-directed CTS frame from the device before sending data. This is the default setting.
  - CTS-RTS—When selected, wireless clients must first send an RTS frame and receive a CTS frame from the device before sending data (a two-frame exchange occurs prior to the actual network transmission).
- CTS Rate—The CTS rate defines the data rate (in Mbps) at which CTS frames are sent. The default rate is 11 Mbps; acceptable values are 1, 2, 5.5, and 11.

## Configuring Short Slots

Short slots, an 802.11g-only feature, can increase efficiency and throughput for wireless traffic. By default, the device supports 802.11g traffic that uses short slots. However, because 802.11b does not support short slots, you might want to disable short slots for all protocols when your wireless network is handling 802.11b traffic.

To disable short slot for 802.11g packets:

1. In the NSM navigation tree, select **Device Manager > Devices**. Double-click the device object to open the device configuration.
2. In the device navigation tree, select **Wireless Settings > Advanced**, and then select **Long** in the Set Slot Time option.

## Configuring Preambles

A preamble is the sequence of bits within a transmission that, when recognized and received by a wireless client, enables the client to locate the remaining packets in the transmission. The preamble length is defined in the Synchronization field of a wireless packet, and can be long or short:

- A long preamble (128 bits) provides the wireless client more time to process the preamble, which can provide greater interoperability with older wireless protocols and non-short-preamble equipment. All 802.11 devices support a long preamble.
- A short preamble (56 bits) can improve efficiency because the client does not spend time processing the preamble. However, older wireless protocols do not support short preambles.

By default, the device does not support long preambles. To enable long preambles for 802.11b packets only:

1. In the NSM navigation tree, select **Device Manager > Devices**. Double-click the device object to open the device configuration.
2. In the device navigation tree, select **Wireless Settings > Advanced**, and then select **Long Transmit Preamble**.

- Related Documentation**
- [Virtual Routers Overview on page 294](#)
  - [Wireless Settings in a Security Device Overview on page 379](#)
  - [Configuring General Wireless Settings on page 380](#)
  - [Configuring Wireless MAC Access Lists on page 387](#)
  - [Configuring Wireless General SSID Settings on page 388](#)
  - [Reactivating Wireless Connections on page 394](#)

## Configuring Wireless MAC Access Lists

The access control list (ACL) controls the wireless clients that can connect to the wireless network. The ACL identifies clients by their MAC addresses and directs the device to permit or deny access for each address. The ACL settings apply globally to all basic service sets (BSSs). The following topics explain different methods to configure ACLs.

### Configuring MAC Access Mode

You can configure the ACL to operate in one of the following modes:

- **Disabled**—When enabled, the security device does not filter MAC addresses. This is the default mode.
- **Enabled**—When enabled, the security device permits access to all hosts except those marked with a Deny control status. Use this option when you want to deny specific hosts, but allow unknown hosts to connect.
- **Strict**—When enabled, the security device denies access to all hosts except those marked with an Allow control status. Use this option when you want to restrict network access to specific hosts.

To configure the ACL mode:

1. In the NSM navigation tree, select **Device Manager > Devices**. Double-click the device object to open the device configuration.
2. In the device navigation tree, select **Wireless Settings > MAC Access List**, and then select the **MAC Access Mode**.

### Configuring MAC Addresses

You can specify a maximum of 128 MAC addresses. To add an address:

1. In the NSM navigation tree, select **Device Manager > Devices**. Double-click the device object to open the device configuration.
2. In the device navigation tree, select **Wireless Settings > MAC Access List**, and then click the Add icon to display the New MAC address dialog box. Configure the following:
  - **MAC Address**—Defines the MAC address of the client.

- Control Status—Defines the action the device takes when a client with the specified MAC address is detected.

For example:

- If the control status is set to Deny and the MAC access mode is set to Strict, the device denies the client.
- If the control status is set to Allow and the MAC access mode is Deny or Strict, the device allows the client to connect.



**NOTE:** NSM does not support the learned MAC address list.

---

**Related  
Documentation**

- [Virtual Routers Overview on page 294](#)
- [Wireless Settings in a Security Device Overview on page 379](#)
- [Configuring General Wireless Settings on page 380](#)
- [Configuring Advanced Wireless Settings on page 383](#)
- [Configuring Wireless General SSID Settings on page 388](#)
- [Configuring SSID Authentication and Encryption on page 389](#)
- [Reactivating Wireless Connections on page 394](#)

---

## Configuring Wireless General SSID Settings

---

To enable wireless clients to connect to the NetScreen-5GT Wireless security device, you must configure at least one basic service set (BSS) that defines and controls how the device handles traffic through a wireless interface.

You can create up to eight basic service sets, but the device can only use a maximum of only four at one time. You might want to configure extra service sets when your network uses site-specific or time-specific BSSs: To enable different BSSs, bind or unbind their corresponding SSIDs to interfaces.

A new SSID does not contain default general settings; you must at least configure a name and select wireless interface for the SSID before the device can handle wireless traffic for that BSS. The general SSID settings are displayed in [Table 89 on page 389](#).



Table 89: Wireless General SSID Settings

Parameters	Your Action
Name	Specify a name that uniquely identifies the BSS. The device uses the SSID name to distinguish the interface to route wireless traffic to. For enhanced security, do not assign the SSID a meaningful name that an attacker might be able to determine through reconnaissance, such as the department or location of the WAP. You can also make the name difficult to guess by using a mix of upper- and lowercase letters, numbers, and symbols. When the SSID name contains one or more spaces, enclose the name within quotation marks.
Suppressing Transmission of SSID Information	Select so the device does not display the SSID name in broadcasts. Because the name is not broadcast, attackers must work harder to obtain the SSID name.
Isolation of Clients on the Same SSID	Select to prevent wireless clients on the same subnetwork (SSID) from communicating directly with each other and bypassing the security device.
Wireless Interface	Select the wireless interface (wireless 1 or wireless 2) that handles traffic for the SSID. The device routes all wireless traffic with the specified SSID name through this interface.

#### Related Documentation

- [Virtual Routers Overview on page 294](#)
- [Configuring General Wireless Settings on page 380](#)
- [Configuring Advanced Wireless Settings on page 383](#)
- [Configuring Wireless MAC Access Lists on page 387](#)
- [Configuring SSID Authentication and Encryption on page 389](#)
- [Reactivating Wireless Connections on page 394](#)

## Configuring SSID Authentication and Encryption

Each SSID can use specific authentication and encryption settings, enabling you to configure differing levels of security for different resources. By default, the authentication/encryption is set to none; **we strongly recommend that you select one of the supported authentication/encryption methods**. The NetScreen-5GT Wireless device supports WEP and WPA authentication and encryption methods; to ensure the highest level of security we recommend that you select WPA as your authentication/encryption method.

The Wired Equivalent Privacy (WEP) uses the Rivest Cipher 4 (RC4) stream cipher algorithm to encrypt and decrypt data as it travels over the wireless link. You can store WEP keys locally on the security device or externally on an external authentication server. Wireless network users store one or more of the same keys on their systems and identify them with the same ID numbers. For details on configuring WEP, see [“Configuring Wired Equivalent Privacy” on page 390](#).

The Wi-Fi Protected Access (WPA) method patches many of the security vulnerabilities found in WEP, greatly enhancing payload integrity checks and the key exchange process. You can use WPA in one of the following modes:

- **WPA Mode**—In this mode, also known as Enterprise Mode, the device uses the Extensible Authentication Protocol (EAP) for authentication through an 802.1X-compliant RADIUS server (such as the OAC RADIUS server and the Microsoft IAS RADIUS server). When handling wireless traffic, the device forwards authentication requests and replies between the wireless clients and the RADIUS server; after successfully authenticating a client, the RADIUS server sends an encryption key to both the client and to the device. The device itself manages the encryption process using Temporal Key Integrity Protocol (TKIP) or Advanced Encryption Standard (AES).
- **WPA-PSK**—In this mode, also known as Personal Mode, the device uses preshared keys (PSKs) or a passphrase for authentication and encryption. Keys are stored on the device and on all wireless clients; you do not need to configure a separate authentication server.



**NOTE:** For details about TKIP, see the IEEE standard 802.11. For details about AES, see RFC 3268, “Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS).”

For details on configuring WPA, see [“Using Wi-Fi Protected Access” on page 393](#).

## Configuring Wired Equivalent Privacy

Although you can configure WEP for all the basic service sets (BSSs), the NetScreen-5GT Wireless device intentionally restricts its use to only one BSS at a time.

- **Auto**—When selected, the device automatically negotiates with wireless clients whether or not the client authenticates itself with a WEP shared key (device accepts both open encryption or shared-key authentication). Use this option to improve compatibility between the WAP and wireless devices using various operating systems that support different implementations of WEP.
- **Open**—When selected, a wireless client must provide the SSID to the device before the device authenticates the client. For encryption, select one of the following:
  - **None**—When selected, no encryption is performed.
  - **WEP**—When enabled, an authenticated wireless client must provide a WEP key to the device before the client can encrypt and decrypt communication over the WLAN. Because the Open option is insecure (especially if the device is configured to broadcast the SSID), we recommend that you also enable WEP encryption.

When using WEP encryption, you must also select a key source, which specifies the location of the WEP key:

- **None or Local**—The key is stored on the security device. This is the default key-source when None is selected. When enabled, you must configure a default WEP key on the security device.

- **Server**—The key is stored on a RADIUS authentication server. When enabled, you must configure a RADIUS authentication server to handle WEP key requests (you do not need to configure or use a WEP key on the security device).
- **Both**—The key is stored on the security device and on the RADIUS authentication server. When enabled, you must configure a RADIUS authentication server to handle WEP key requests and configure a default WEP key on the security device.
- **Shared Key**—When selected, both the device and the wireless clients use the same key for authentication and encryption/decryption. You must configure a default WEP key on the security device.

During a shared key exchange:

- a. The wireless client contacts the device.
- b. The device responds to the client with a clear-text challenge text string that the client must then encrypt with the correct WEP key and return to the device.
- c. The device receives the encrypted string from the client, decrypts it, and compares it with the original. If the strings match, authentication is successful; if the strings do not match or the client does not respond, authentication fails.

Although this method uses WEP keys for encryption, an attacker might be able to intercept both the clear-text challenge and the same challenge encrypted with a WEP key, and potentially decipher the WEP key.

## Configuring WEP Keys

You can define WEP keys on the security device for BSS use. The security device, acting as a wireless access point (WAP), uses WEP keys for authenticating wireless clients in that BSS, and for encrypting and decrypting traffic sent between itself and the clients.

You can define one to four WEP keys for each BSS on the security device. Using multiple keys enables you to adjust the level of security for different wireless clients within the same BSS; you can use longer keys to provide greater security for some traffic and smaller keys to reduce processing overhead for other, less critical traffic.

When you define only one WEP key on the security device, that key is the default key and handles all encryption, authentication, and decryption. When you define multiple keys on the security device, you can designate non default keys to handle authentication and decryption (the default key always handles encryption). If you do not specify a default key, the first key you define automatically becomes the default key.

Wireless clients can use a static WEP key stored on the device, or a dynamic key on an external RADIUS server.

- When clients use a unique, dynamic WEP key from an external RADIUS server, the security device also uses this unique key—which it also receives from the RADIUS server—for bidirectional communication.

- When clients use static WEP keys stored locally on the security device, the device uses the default key to encrypt all transmitted wireless traffic. Clients must also have the default key loaded to decrypt traffic from the device.

The Key ID enables WEP key configuration and sets the WEP identification value. When all WEP keys are stored on the security device, you can assign the default key ID as 1, 2, 3, or 4.

However:

- When using WEP keys stored on the security device and dynamic WEP keys created by an external RADIUS server (RADIUS dynamically creates and distributes a different key per session for each wireless client), the ID for the default WEP key on the security device cannot be 1 because the RADIUS server uses 1 as the ID for all its keys. The security device can use a default WEP key with key ID 2, 3, or 4 for encryption, and a different WEP key with ID 1, 2, 3, or 4 for authentication and decryption.
- When all WEP keys are on an external RADIUS server, the server uses a key ID of 1 for all its keys (RADIUS dynamically creates and distributes a different key per session for each wireless client).

An encryption key length specifies the length of the key in bits. Juniper Networks supports two WEP key lengths: 40 and 104 bits. Because the keys are concatenated with a 24-bit initialization vector (IV), the resulting lengths are 64 and 128 bits.

Longer keys are more secure than shorter keys, but longer keys take longer to process and can reduce throughput speeds. Select the key length that is appropriate to the importance of the wireless traffic you want to protect:

- 40-bit—A 40-bit encryption length enables you to enter 10 hexadecimal digits or 5 ASCII characters.
- 104-bit—A 104-bit encryption length enables you to enter 26 hexadecimal digits or 13 ASCII characters.

The encryption method defines the string type (ASCII or hexadecimal) for the WEP key:

- ASCII—Plain text string.
  - When using 40-bit length and ASCII method, enter 5 ASCII characters.
  - When using a 104-bit length and ASCII method, enter 13 ASCII characters.
- Hexadecimal (default)—A hexadecimal string uses only A-F characters and 0-9 numbers. For example, 662ADC918DDD662ADC918DDD66 is a valid hexadecimal string but CADETS01234567890123456789 is not; the T and S are outside the valid hexadecimal range. The number of hexadecimal characters you enter depends on the specified key length:
  - When using 40-bit length and hexadecimal method, enter 10 hexadecimal characters.
  - When using a 104-bit length and hexadecimal method, enter 26 hexadecimal characters.

When using a single key on the security device for encryption, decryption, and authentication, you must define the default WEP key.

You can specify a static, non default WEP key that the security device uses for authenticating and decrypting traffic received from wireless clients. However, each client must also load the WEP key (and ID) before they can authenticate themselves and send encrypted traffic to the security device. If a client does not supply a key ID, the security device attempts to use the default WEP key to authenticate the client and decrypt its traffic.

## Using Wi-Fi Protected Access

You can configure the SSID to use WPA enterprise mode or WPA personal mode.

WPA (Enterprise Mode) authentication uses an external RADIUS auth server for authentication. When using WPA, you must also configure the rekey interface and encryption method. The WPA enterprise mode settings are displayed in [Table 90 on page 393](#).

**Table 90: WPA Enterprise Mode Settings**

Parameters	Description
Encryption	<p>The encryption setting specifies the encryption method used between the security device and wireless clients in the subnetwork. Select one of the following:</p> <ul style="list-style-type: none"> <li>• AES—The Advanced Encryption Standard (AES) is used by WPA 2 devices. AES uses the Robust Security Network (RSN) cipher for encryption. This complex encryption mechanism is a block cipher (operates on 128 bit data blocks).</li> <li>• TKIP—The Temporal Key Integrity Protocol (TKIP) is used by WPA 1 devices. TKIP is a key management protocol that handles key generation and key synchronization; TKIP uses the RC4 algorithm for encryption.</li> <li>• Auto—When enabled, the device uses the encryption method (AES or TKIP) used by the client.</li> </ul>
rekey-interval	<p>The rekey interval defines the number of seconds between group key updates. To enable key updates, select <b>Value</b>; the default interval is 1800 seconds and the acceptable range is 30-42949672 seconds. To disable key updates, select <b>Disabled</b>.</p>

WPA-PSK (Personal Mode) authentication uses a passphrase or pre shared key on the security device to permit access to the SSID. When using WPA, you must also configure the WPA-PSK authentication and encryption methods. The WPA personal mode settings are displayed in [Table 91 on page 394](#).

Table 91: WPA Personal Mode Settings

Parameters	Description
Authentication (WPA-PSK)	<p>The authentication setting specifies the authentication methods for wireless clients attempting to access the SSID:</p> <ul style="list-style-type: none"> <li>Passphrase—When enabled, you must configure a passphrase (8-63 ASCII characters) that permits access to the SSID.</li> <li>PSK—When enabled, you must enter a pre shared key (256 bit/64characters hexadecimal) that permits access to the SSID.</li> </ul>
Encryption	<p>The encryption setting specifies the encryption method used between the security device and wireless clients in the subnetwork. Select one of the following:</p> <ul style="list-style-type: none"> <li>AES—The Advanced Encryption Standard (AES) is used by WPA 2 devices. AES uses the Robust Security Network (RSN) cipher for encryption. This complex encryption mechanism is a block cipher (operates on 128 bit data blocks).</li> <li>TKIP—The Temporal Key Integrity Protocol (TKIP) is used by WPA 1 devices. TKIP is a key management protocol that handles key generation and key synchronization; TKIP uses the RC4 algorithm for encryption.</li> <li>Auto—When enabled, the device uses the encryption method (AES or TKIP) used by the client.</li> </ul>

#### Related Documentation

- [Virtual Routers Overview on page 294](#)
- [Configuring General Wireless Settings on page 380](#)
- [Configuring Advanced Wireless Settings on page 383](#)
- [Configuring Wireless MAC Access Lists on page 387](#)
- [Configuring Wireless General SSID Settings on page 388](#)
- [Reactivating Wireless Connections on page 394](#)

## Reactivating Wireless Connections

When you make changes to the wireless settings on the security device, you must update the device with your changes before the new settings take effect.



**NOTE:** When using an authentication server for wireless authentication, if you enable 802.1X support on that server, you must also reactive the WLAN subsystem before the change can take effect.

Additionally, the device must reactivate its WLAN subsystem to use the new settings. NSM automatically reactivates the WLAN subsystem within the NetScreen-5GT Wireless security device during the device update process.

The reactivation process takes several seconds (approximately 10 seconds) to complete. During reactivation of the WLAN subsystem, the device severs all wireless connections

and clears all wireless sessions from the session table. Previously connected wireless clients must reconnect to reestablish their disrupted sessions.

**Related  
Documentation**

- [Virtual Routers Overview on page 294](#)
- [Configuring General Wireless Settings on page 380](#)
- [Configuring Advanced Wireless Settings on page 383](#)
- [Configuring Wireless MAC Access Lists on page 387](#)
- [Configuring Wireless General SSID Settings on page 388](#)

---

## Conducting a Site Survey for Detecting Access Points

When setting up the NetScreen-5GT Wireless (ADSL) device as a wireless access point (WAP), you can scan the broadcast vicinity to see if there are any other WAPs broadcasting nearby. A site survey detects any WAPs emitting a beacon in its area and records the following details about each detected WAP:

- Service set identifier (SSID)
- MAC address
- Received signal strength indicator (RSSI) The RSSI numbers are in decibels (dBs) that indicate the signal-to-noise ratio (SNR). The SNR is the signal level divided by the noise level, which results in a value representing signal strength.
- Broadcast channel

In addition to performing an initial site survey, you might want to perform occasional surveys to ensure that no rogue WAPs are operating in the area.

A site survey takes about 5-10 seconds to complete.

**Related  
Documentation**

- [Wireless Settings in a Security Device Overview on page 379](#)
- [Network, Interface, and Security Modules Supported in Security Devices on page 395](#)
- [WPA2, Extended Range, and Super G Support on NetScreen5GT Wireless Overview on page 399](#)
- [Configuring General Wireless Settings on page 380](#)
- [Configuring Advanced Wireless Settings on page 383](#)

---

## Network, Interface, and Security Modules Supported in Security Devices

This topic includes information about how to configure network module, slot information in security devices, and various physical interface modules that are supported by security devices.

## Configuring the Network Module

Some security device systems, such as the NetScreen-500, NetScreen 5000 line, and ISG Series, contain physical slots in which you can install optional modules.

The NetScreen 5000 line running ScreenOS 6.1 or later supports three cards MGT3, 8G2-G4, and 2XGE-G4. These cards need to use M3A-Management\_Module, which is a special image for NetScreen 5000 line devices. Also, the ISG1000 and ISG2000 running ScreenOS 6.1 or later support a new 10Gb interface slot that large enterprise and service provider customers require.

## Slot Information in Security Devices

- **Physical Interface Modules**—The SSG520 and SSG550 security devices use WAN data links to transmit and receive traffic across geographically dispersed networks. You define the properties of the data link by configuring the WAN interface that corresponds to a port on an SSG Physical Interface Module (PIM).
- **Copper and Fiber Interface Modules**—These modules provide additional Ethernet ports.
- **Management Modules**—These modules provide management functionality for the ISG2000 and ISG1000 devices. The NetScreen 5000 line network modules are known as Secure Port Modules (SPMs); SPMs handle general packet processing at gigabit speeds, enabled by ASIC support.



**NOTE:** On SSG520 and SSG550 security devices only, slot 0 is reserved for the device motherboard. The card type is referred to as “4 Ethernet interfaces (10/100/1000) fixed.”

The Chassis screens provide additional information about network modules installed in the available chassis slots of an ISG1000 or ISG2000 security device. The information displayed in the Chassis screens, including the version and serial number of the card, is obtained from the card installed in the physical device and is read-only.

You must configure the network module before physical interfaces appear in the NSM UI (even for imported devices).

## Physical Interface Modules Supported by SSG520 and SSG550 Security Devices

The WAN interface type PIMs that are supported by SSG520 and SSG550 devices are displayed in [Table 92 on page 396](#):

**Table 92: PIMs Supported by SSG520 and SSG 550 Security Devices**

Parameters	Description
Serial	Serial PIMs on SSG devices have two serial ports per PIM, which support full-duplex, synchronous data transmission. These ports can transmit packets at speeds up to 8 Mbps. You cannot use these serial ports to connect a console or modem.



**Table 92: PIMs Supported by SSG520 and SSG 550 Security Devices (*continued*)**

Parameters	Description
T1	T1 PIMs on SSG devices contain two T1 ports with integrated channel service unit/data service unit (CSU/DSU). These ports provide physical connections to T1 or fractional T1 network media types.
E1	E1 PIMs on SSG devices have two E1 ports with integrated CSU/DSU. These ports provide physical connections to E1 or fractional E1 network media types.
T3 (also known as DS3)	Digital signal level 3 (DS3) PIMs on SSG devices contain one physical DS3 port with integrated DSU. This port provides physical connection to T3 network media types at a bit rate of 44.736 Mbps.

## Interface Modules (Copper)

A single security device can support a 10/100Base-T and GBIC card simultaneously; however, the cards are not hot-swappable.

### 10/100 Mbps

The 10/100 Mbps interface module is typically used to support a 10Base-T or 100Base-T LAN. The card can support 2, 4, or 8 copper interfaces, and uses RJ-45 connectors with twisted pair.



**NOTE:** The ISG2000 supports a maximum port count of 28. When using 8-port 10/100-Mbps modules in each I/O slot, ports five through eight in slot 4 are automatically disabled. You cannot configure these ports for firewall or HA functionality.

### 10/100/1000 Mbps

The tri-mode card, available for ISG security devices, is a 2 Ethernet port 10/100/1000-Mbps I/O card. The card supports 2 copper interfaces, uses RJ-45 connectors and twisted pair, and contains the following I/O port configurations:

- 10-Mbps full/half duplex
- 100-Mbps full/half duplex
- 1000-Mbps full duplex
- Auto (autonegotiate link speed/duplex)

## Interface Modules (Fiber)

The fiber interface module provides connectivity for fiber-based, Gigabit Ethernet LANs.

- Gigabyte

- 1 interface (mini-GBIC)—This card supports 1 fiber interface and uses an optical cable with SX or LX connectors.
- 2 interfaces (GBIC)—This card supports 2 fiber interfaces and uses an optical cable with SX or LX connectors.
- Gigabyte LX/SX (2 interfaces)—This card supports 2 fiber interfaces and uses an optical cable with SX and LX connectors.

## Secure Port Modules

Secure Port Modules (SPMs) provide general packet processing and device connection tasks for the NetScreen 5000 line. These modules are based on either the GigaScreen-II or Jupiter-II ASIC.

SPMs handle packets as they enter and exit the system, providing packet parsing, classification, and flow-level processing. SPMs also provide encryption, decryption, Network Address Translation (NAT), and session lookup features. When packets require additional processing, the device forwards the packets to the management module.

The SPMs for the NetScreen 5000 line of security devices supported by NSM are displayed in [Table 93 on page 398](#).

**Table 93: SPMs Supported by NSM**

Parameters	Description
5000-8G SPM	This SPM provides eight 1-Gigabit Ethernet mini-Gigabit Interface Connector (GBIC) ports using hot-swappable transceivers. The 5000-8G SPM delivers up to 4 Gbps of firewall and up to 2 Gbps of VPN capacity. This module is also capable of supporting a total of four aggregate interfaces. The 5000-8G SPM provides port Link and Activity LEDs in addition to Power and Status LEDs.
5000-8G2 SPM	This SPM provides eight 1-Gigabit Ethernet mini-GBIC ports using hot-swappable transceivers. The 5000-8G2 SPM delivers up to 8 Gbps of firewall and up to 4 Gbps of VPN capacity. This module is also capable of supporting a total of four aggregate interfaces, with up to four ports for each aggregate interface. The 5000-8G2 SPM provides port Link and Activity LEDs in addition to Power and Status LEDs.
5000-2G24FE SPM	This SPM provides two 1-Gigabit Ethernet ports and 24 FE ports with up to 2 Gbps of firewall and up to 1 Gbps of VPN process capacity. This module is capable of supporting a total of six aggregate interfaces. This total consists of one aggregate interface for the two 1-Gigabit ports, and five aggregate interfaces for the 24 10/100 Ethernet ports. Only similar ports can be aggregated together. You cannot aggregate a gigabit port to a 10/100 FE port. The 5000-2G24FE SPM provides port Link and Activity LEDs, in addition to Power and Status LEDs. Mini-GBIC transceivers are hot-swappable.
5000-2XGE SPM	This SPM provides two 10-Gigabit Ethernet ports using hot-swappable 10-Gigabit Small Form Factor Pluggable Module for PHY transceiver. The 5000-2XGE SPM delivers up to 10 Gbps of firewall and up to 5 Gbps of VPN capacity. This module provides port Link and Activity LEDs in addition to Power and Status LEDs.

- Related Documentation**
- [Wireless Settings in a Security Device Overview on page 379](#)
  - [Chassis Information Overview on page 399](#)
  - [WPA2, Extended Range, and Super G Support on NetScreen5GT Wireless Overview on page 399](#)
  - [Conducting a Site Survey for Detecting Access Points on page 395](#)

---

## Chassis Information Overview

For ISG series security devices, you can view read-only information about the modules installed in the chassis of the device.

By default, the chassis includes a management module.

For ISG series security devices running ScreenOS 5.0.0-IDP1, or ScreenOS 5.4 or later, the chassis also includes the IDP series security module.

- Related Documentation**
- [Wireless Settings in a Security Device Overview on page 379](#)
  - [Network, Interface, and Security Modules Supported in Security Devices on page 395](#)
  - [WPA2, Extended Range, and Super G Support on NetScreen5GT Wireless Overview on page 399](#)
  - [Wi-Fi Protected Access Overview on page 400](#)
  - [Conducting a Site Survey for Detecting Access Points on page 395](#)

---

## WPA2, Extended Range, and Super G Support on NetScreen5GT Wireless Overview

WPA2 is the second generation of WPA security. WPA2 is based on the final IEEE 802.11i amendment to the 802.11 standard. One of the primary improvements in WPA2 is stronger encryption.

Extended Range improves WLAN infrastructure in coverage that is required for connectivity at long ranges and in all corners of the home, office, enterprise, or hot spot.

Super G dramatically increases throughput needed for bandwidth intensive application and growing volume of users. By bonding two 54 Mbps channels, it delivers significantly higher throughput (up to 108mbps) versus .11b, .11g, and .11a technologies.

- Related Documentation**
- [Wireless Settings in a Security Device Overview on page 379](#)
  - [Network, Interface, and Security Modules Supported in Security Devices on page 395](#)
  - [Chassis Information Overview on page 399](#)
  - [Wi-Fi Protected Access Overview on page 400](#)
  - [Conducting a Site Survey for Detecting Access Points on page 395](#)

## Wi-Fi Protected Access Overview

---

Wi-Fi Protected Access (WPA) is a more secure solution for WLAN authentication and encryption and was designed in response to many of the weaknesses in WEP. NSM supports WPA and WPA2.

WPA and WPA2 support 802.1X authentication, which use an Extensible Authentication Protocol (EAP) method for authentication through a RADIUS server. EAP is an encapsulation protocol used for authentication and operates at the Data Link Layer (Layer 2). For more information, refer to RFC 2284, *PPP Extensible Authentication Protocol (EAP)*.

When using WPA or WPA2 with a RADIUS server, the security device forwards authentication requests and replies between the wireless clients and the RADIUS server. After successfully authenticating a client, the RADIUS server sends an encryption key to the client and the security device. From that point, the security device manages the encryption process, including the encryption type—Temporal Key Integrity Protocol (TKIP) or Advanced Encryption Standard (AES)—and the rekey interval. For information about TKIP, see the IEEE standard 802.11. For information about AES, see RFC 3268, *Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)*.

You can also use WPA or WPA2 with a preshared key, which is a static key that is configured on the security device and the client's device. Both devices use the key to generate a unique key (group key) for the session. You can specify the preshared key by using an ASCII passphrase (password) or in hexadecimal format. You also use the same encryption types as with 802.1X authentication: TKIP or AES.

### Related Documentation

- [Wireless Settings in a Security Device Overview on page 379](#)
- [Network, Interface, and Security Modules Supported in Security Devices on page 395](#)
- [Chassis Information Overview on page 399](#)
- [WPA2, Extended Range, and Super G Support on NetScreen5GT Wireless Overview on page 399](#)
- [Conducting a Site Survey for Detecting Access Points on page 395](#)

## Configuring Wi-Fi Protected Access (NSM Procedure)

---

To configure Wi-Fi protected access:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Select a security device and then double-click the device on which you want to define forced timeout. The device configuration appears.
3. In the device navigation tree, select **Wireless**.
4. Configure the following wireless settings:

- For Select Specific Antenna, select **Antenna diversity**
  - For Channel for wireless AP radio, select **Auto**.
  - For Operation mode for AP, select **802.11b/g**.
  - For Transmit Power, select **Full**.
  - For Data Rate for AP, select the best rate.
  - In the main navigation tree, select **Wireless>SSID**.
5. Select **New** and configure the following settings:
- For Name, enter **my-ssid**.
  - For Wireless Interface, select **wireless 2**.
  - For Authentication/Encryption, select **WPA2**.
  - For Select Encryption Method, select **Auto**.
  - For auth-server-name, select **rd\_1\_1\_1**.
  - For Rekey Interval, select **None**. Rekey interval is the time that elapses before the group key for clients is updated.
6. Configure the following WPA2-PSK settings:
- For Authentication/Encryption, select **WPA2-PSK**.
  - For WPA2-PSK, select **Passphrase**. When enabled, you must configure a passphrase (8-63 ASCII characters) that permits access to the SSID.
  - For Passphrase, set a password.
  - For Encryption Method, select **TKIP**.
  - For Rekey Interval, select **Value**.
  - For Value, select a value. 1800 is the default.
  - Click **OK** to apply the settings.

#### Related Documentation

- [Wireless Settings in a Security Device Overview on page 379](#)
- [Network, Interface, and Security Modules Supported in Security Devices on page 395](#)
- [Chassis Information Overview on page 399](#)
- [WPA2, Extended Range, and Super G Support on NetScreen5GT Wireless Overview on page 399](#)
- [Wi-Fi Protected Access Overview on page 400](#)
- [Conducting a Site Survey for Detecting Access Points on page 395](#)

## Super G Methods Overview

---

In wireless devices that have an Atheros Communications chipset with the Super G feature, you can enable Super G, which can increase the user data throughput rate up to 4 Mbps for 802.11a and 802.11g clients by using the following methods:

- Bursting—Allows the device to transmit multiple frames in a burst rather than pausing after each frame.
- Fast frames—Allows more information per frame to be transmitted by allowing a larger-than-standard frame size.
- Compression—Allows link-level hardware compression to be performed by a built-in data compression engine.

By default, this feature is disabled.

If wireless clients do not support Super G and the security device has Super G enabled, they can still connect to the wireless network, but the Super G feature is not available.



**NOTE:** You can read more about Atheros Communications Super G chipset at [www.atheros.com](http://www.atheros.com).

---

### Related Documentation

- [Wireless Settings in a Security Device Overview on page 379](#)
- [Network, Interface, and Security Modules Supported in Security Devices on page 395](#)
- [WPA2, Extended Range, and Super G Support on NetScreen5GT Wireless Overview on page 399](#)
- [Reactivating Wireless Connections on page 394](#)

## Configuring Atheros XR (NSM Procedure)

---

You can enable Atheros Communications eXtended Range (XR) technology. XR processes 802.11 signals, defined by IEEE 802.11a and 802.11g standards, so that wireless networks have fewer “dead spots” and greater range than usual. XR processes weaker signals more effectively and allows greater coverage. XR provides increased coverage at a lower data transmission rate.

Only the first active SSID per radio can support XR. When XR is enabled, the first active SSID per radio uses the XR feature.

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Select a security device and then double-click the device on which you want to define forced timeout. The device configuration appears.
3. In the device navigation tree, select **Wireless**.
4. Configure the following settings:

- For Select Specific Antenna, select **Antenna Diversity**.
  - For Channel for wireless AP radio, select **Auto**.
  - For Operation mode for AP, select **802.11b/g**.
  - For Transmit Power, select **Full**.
  - For Data Rate for AP, select the best rate.
  - Select **Enable SuperG**. If the security device has more than one radio, make the selection for the radio you want.
  - Select **XR Support**. If the security device has more than one radio, make the selection for the radio you want.
  - Click **OK** to apply the settings.
  - In the main navigation tree, select **Wireless>SSID**.
5. Select New and configure the following settings:
- For Name, enter **my-ssid**.
  - For Wireless Interface, select **wireless 2**.
  - For Authentication/Encryption, select **None**.
  - Click **OK** to apply the settings.

For detailed information on these WLAN features, see the *Concepts & Examples ScreenOS Reference Guide*.

#### Related Documentation

- [Wireless Settings in a Security Device Overview on page 379](#)
- [Network, Interface, and Security Modules Supported in Security Devices on page 395](#)
- [WPA2, Extended Range, and Super G Support on NetScreen5GT Wireless Overview on page 399](#)
- [Super G Methods Overview on page 402](#)
- [Reactivating Wireless Connections on page 394](#)
- [Conducting a Site Survey for Detecting Access Points on page 395](#)





# General Packet Radio Service

General Packet Radio Service (GPRS) networks connect to several external networks including those of roaming partners, corporate customers, GPRS Roaming Exchange (GRX) providers, and the public Internet. GPRS network operators face the challenge of protecting their network while providing and controlling access to and from these external networks. Juniper Networks provides solutions to many of the security problems plaguing GPRS network operators.

In the GPRS architecture, the fundamental cause of security threats to an operator's inherent lack of security in GPRS Tunneling Protocol (GTP). GTP is the protocol used between GPRS support nodes (GSNs). Communication between different GPRS networks is not secure because GTP does not provide any authentication, data integrity, or confidentiality protection. Implementing Internet Protocol Security (IPsec) for connections between roaming partners, setting traffic rate limits, and using stateful inspection can eliminate a majority of the GTP's security risks. Juniper Networks security devices mitigate a wide variety of attacks on the Gp, Gn, and Gi interfaces.



**NOTE:** Only ISG2000 devices support GTP functionality. For more information on GPRS, see the *Concepts and Examples ScreenOS Reference Guide*.

This chapter contains the following topics:

- [3GPP R6 Information Elements Support Overview on page 405](#)
- [Configuring Access Point Name Restriction \(NSM Procedure\) on page 407](#)
- [Configuring IMSI Prefix Filter \(NSM Procedure\) on page 407](#)
- [DHCP Relay Overview on page 408](#)

## 3GPP R6 Information Elements Support Overview

Information elements (IEs) are included in all GTP control message packets. IEs provide information about GTP tunnels, such as creation, modification, deletion, and status. NSM supports IEs consistent with Third-Generation Partnership Project (3GPP) Release 6. If you are running an earlier release, or have contractual agreements with operators running earlier releases of 3GPP, you can reduce network overhead by restricting control messages containing unsupported IEs.

In 3GPP R6, the following new IEs have been added:

- [Radio Access Technology on page 406](#)
- [Routing Area Identity and User Location Information on page 406](#)
- [APN Restriction on page 406](#)
- [IMSI Prefix Filtering on page 406](#)
- [IMEI-SV on page 406](#)

## Radio Access Technology

The Radio Access Technology (RAT) information element provides ways to stimulate Wideband Code Division Multiple Access (WCDMA) and to perform reporting through billing information systems.

## Routing Area Identity and User Location Information

Some countries restrict subscriber access to certain types of network content. To comply with these regulatory demands, network operators need to be able to police subscriber's requested content before allowing a content download. NSM gives network operators the ability to screen content based on the Routing Area Identity (RAI) and User Location Information (ULI) IEs.

## APN Restriction

Multiple concurrent primary packet data protocol (PDP) contexts, and an MS/UE capable of routing between these two access points, can put IP security at risk for corporate users who have both private and a public APN. The APN Restriction IE, added to the GTP **create PDP context** response message, ensures the mutual exclusivity of a PDP context if requested by a GGSN (or rejected if this condition cannot be met), and thus avoids the security threat.

## IMSI Prefix Filtering

A GPRS support node (GSN) identifies a mobile station (MS) by its International Mobile Station Identity (IMSI). An IMSI comprises three elements: the Mobile Country Code (MCC), the Mobile Network Code (MNC), and the Mobile Subscriber Identification Number (MSIN). The MCC and MNC combined constitute the IMSI prefix and identify the mobile subscriber's home network, or Public Land Mobile Network (PLMN). By setting IMSI prefixes, you can configure the security device to deny GTP traffic coming from nonroaming partners. By default, a security device does not perform IMSI prefix filtering on GTP packets. By setting IMSI prefixes, you can configure the security device to filter **create pdp request messages** and permit only GTP packets with IMSI prefixes that match the ones you set. For more information on IMSI prefix filtering, see the *Concepts & Examples ScreenOS Reference Guide*.

## IMEI-SV

The International Mobile Equipment Identity-Software Version (IMEI-SV) IE provides ways to adapt content to the terminal type and client application whenever a proxy server for this purpose is not present. This IE is also useful in reports generated from the GGSN, AAA, and/or Wireless Application Protocol gateway (WAP). The GTP-aware security

device supports the RAT, RAI, ULI, APN Restriction, and IMEI-SV in GTP attributes to avoid treatment or categorization as unambiguous traffic, which can be harmful to GPRS traffic or GPRS roaming traffic. These attributes are included in the set of useful filter attributes used to block specific GPRS traffic and/or GPRS roaming traffic. When you set an IMEI-SV IE, you must also specify an APN.

- Related Documentation**
- [Route Types Overview on page 293](#)
  - [DHCP Relay Overview on page 408](#)
  - [Configuring Access Point Name Restriction \(NSM Procedure\) on page 407](#)

## Configuring Access Point Name Restriction (NSM Procedure)

To configure APN restriction:

1. In the NSM navigation tree, select **Object Manager>GTP Objects**.
2. Select an object and click **Edit**.
3. In the GTP object navigation tree, select **IMSI Prefix and APN Filtering**.
4. Click **New** and specify the following:
  - For APN, enter access point name **mobiphone.com.mnc123.mcc456.gprs**.
  - For Selection Mode, select **Network**.
  - Click **OK** to apply the settings.

- Related Documentation**
- [Route Types Overview on page 293](#)
  - [3GPP R6 Information Elements Support Overview on page 405](#)

## Configuring IMSI Prefix Filter (NSM Procedure)

To configure IMSI prefix filtering:

1. In the NSM navigation tree, select **Object Manager>GTP Objects**.
2. Select an object and click **Edit**.
3. In the GTP object navigation tree, select **IMSI Prefix and APN Filtering**.
4. Click **New** and specify the following:
  - For APN, enter access point name **mobiphone.com.mnc123.mcc456.gprs**.
  - For Selection Mode, select **Mobile Station, Network, Verified**.
  - For MCC-MNC (Mobile Country Code-Mobile Network Code), select **MCC-MNC** and enter **246565**.
  - Click **OK** to apply the settings.

- Related Documentation**
- [Route Types Overview on page 293](#)
  - [3GPP R6 Information Elements Support Overview on page 405](#)
  - [DHCP Relay Overview on page 408](#)
  - [Configuring Access Point Name Restriction \(NSM Procedure\) on page 407](#)

---

## DHCP Relay Overview

Dynamic Host Configuration Protocol (DHCP) was designed to reduce the demands on network administrators by automatically assigning the TCP/IP settings for the hosts on a network. Some security devices can also act as DHCP relay agents, receiving DHCP information from a DHCP server and relaying that information to hosts on any physical or VLAN interface in any zone.

When acting as a DHCP relay agent, the security device forwards DHCP requests and assignments between DHCP clients directly attached to one interface and one or more DHCP servers accessible through another interface. The clients and servers may be in the same security zone or in separate security zones.

You can configure a DHCP relay agent on one or more physical or VLAN interfaces on a security device, but you cannot configure a DHCP relay agent and DHCP server or client functions on the same interface.

When the security device functions as a DHCP relay agent, its interfaces must be in either Route mode or function as a Layer 3 device. For interfaces in Layer 3 mode (that is have IP addresses assigned to the interfaces), you must configure a security policy (from zone to zone or intrazone) to permit the predefined service DHCP Relay before forwarding occurs.

You can configure up to three DHCP servers for each DHCP relay agent. The relay agent unicasts an address request from a DHCP client to all configured DHCP servers. The relay agent forwards to the client all DHCP packets received from all servers. For more information on DHCP configuration, see the *Concepts & Examples ScreenOS Reference Guide*.



**NOTE:** When a security device acts as a DHCP relay agent, the device does not generate DHCP allocation status reports because the remote DHCP server controls all the IP address allocations.

---

- Related Documentation**
- [Route Types Overview on page 293](#)
  - [3GPP R6 Information Elements Support Overview on page 405](#)

## PART 2

# Index

- [Index on page 411](#)



# Index

## Symbols

3GPP R6 IE support.....	405
802.11b support.....	382
802.11g support.....	382

## A

access lists	
configuring.....	296
access lists on WAP.....	387
ACLs on WAP.....	387
admins.....	353
ADSL	
configuring backup link on device.....	92
configuring interface.....	88
connecting the cable.....	89
ISP settings.....	89
LLC multiplexing.....	90
multiplexing mode.....	90
operating mode (DMT).....	90
operating mode, ANSI T1.413 Issue 2.....	90
operating mode, ITU 992.2 (G.lite).....	90
operating mode, ITU G.992.1.....	90
supported port modes.....	91
VC multiplexing.....	90
VPI/VCI settings.....	90
advanced device options.....	112
advanced network settings	
ARP cache.....	108
DIP options.....	109
VIP options.....	108
AES	
about.....	393
aggregate interface.....	77
aging settings on WAP.....	383
aging, configuring on device.....	128
ALG.....	284
configuring on device.....	121
SIP.....	279
ALGs, configuring.....	28
american encryption standard See AES	
ANSI T1.413 Issue 2.....	90

antenna settings on WAP.....	381
ARP cache, configuring on device.....	108
asset recovery.....	155
attack object database	
configuring on device.....	183
attack objects	
disabling on device.....	183
Audit Log Viewer	
about.....	16
authentication	
for device administrators.....	149
NSRP.....	362
Authentication and Encryption.....	400
auto-exporting routes.....	301
AV	
configuring internal scanner.....	176
Scan Manager.....	176

## B

backup link for adsl interface.....	92
banners, configuring on device.....	164
basic service sets on WAP.....	388
beacon settings on WAP.....	384
BGP	
about.....	325
configuring aggregate addresses.....	327
configuring neighbors and peer groups.....	328
configuring networks.....	327
configuring on device.....	325
configuring route maps.....	328
route attributes.....	327
blacklist, configuring.....	27
BSS.....	388
burst settings on WAP.....	384

## C

CA certificates, configuring on device.....	271
certificates	
certificate request.....	267
configuring on device.....	265
CRLs.....	273
imported certificates.....	273
installing certificates.....	269
local certificates.....	266
PKI defaults.....	274
revocation settings.....	275
SCEP.....	270, 271, 275
viewing CA certificates.....	271
X509 certificates.....	274

channel settings on WAP.....	381	device advanced settings	
CLI banners, configuring on device.....	158	about.....	112
CLI management.....	153	host and domain name.....	130
configuring		packet flow.....	122
Atheros XR.....	402	predefined service timeouts.....	115
SuperG.....	402	TFTP/FTP server.....	130
connection attempts, max.....	154	traffic shaping.....	119
console-only restrictions.....	156	device certificate options	
control frame protection settings on WAP.....	385	about.....	265
CTS/RTS settings.....	385	CA certificates.....	271
customer support.....	xviii	certificate request.....	267
contacting JTAC.....	xviii	CRLs.....	273
		imported certificates.....	273
		local certificates.....	266
		PKI defaults.....	274
		SCEP.....	270, 271, 275
		X509 certificates.....	274
<b>D</b>		device configuration	
data rate settings on WAP.....	383	about.....	25
demand circuit, configuring for tunnel		memory optimization.....	26
interface.....	316	device groups	
destination routing table.....	305	using.....	33
device administration		device interface settings	
about.....	146	DHCP.....	58
CLI management.....	153	DIPs.....	67
CLI management, asset recovery.....	155	GRE.....	62
CLI management, CLI banners.....	158	MIPs.....	62
CLI management, configuring SSH.....	156	NAT.....	62
CLI management, console-only		secondary IP.....	61
restrictions.....	156	VIPs.....	65
CLI management, file format.....	153	Device Manager module.....	16, 37
CLI management, max connection		device network settings	
attempts.....	154	dynamic routing protocols.....	311
CLI management, reset hardware		virtual routers.....	292, 359, 400
(device).....	155	device NSRP options	
CLI management, restricting password		about.....	361
length.....	154	active/active.....	368
CLI management, SSH and Telnet ports.....	154	master/backup.....	371
configuring HTTP.....	159	synchronizing.....	369
configuring SSL.....	160	device reporting options	
date/time.....	161	email notification.....	167
device admins, authentication method.....	149	general.....	166
device admins, passwords.....	150	NSM.....	167
device admins, privilege levels.....	148	SNMP.....	167
device admins, public key authentication		syslog.....	167
(PKA).....	150	WebTrends.....	168
device admins, root.....	148	device security options	
disabling SSL on device.....	161	disabling attack objects.....	183
permitted IPs.....	152	Web filtering.....	188
secondary banner.....	158		
Web management.....	159		
device administrator			
configuring root.....	148		



device vsys options	
about.....	248
interfaces.....	251
virtual routers.....	248
zones.....	249
DHCP	
configuring in device.....	58
custom DHCP options.....	59
relay agent.....	408
DHCP enhancement.....	353
DIP groups, configuring.....	100
DIP options, configuring on device.....	109
DIP translation stickiness.....	109
DIPs	
configuring in device.....	67
extended interface.....	69
incoming DIP for SIP.....	73
port translation.....	68
discrete multitone.....	90
diversity antennas.....	381
DMT.....	90
DNS	
configuring on device.....	103
dynamic DNS, configuring on device.....	106
proxy, configuring on device.....	104
DNS reply without matched request, allow.....	123
DSCP class selector.....	120
DSL.....	136
dynamic DNS.....	106
dynamic routing protocols	
about.....	311
BGP.....	325
OSPF.....	311
RIP.....	319
<b>E</b>	
ECMP routes, configuring maximum on virtual	
router.....	295
email notification, configuring on device.....	167
encrypting NSRP traffic.....	362
expanded VPN view.....	195
export rules	
configuring on virtual router.....	300
external AV scanner	
about.....	175
fail mode traffic permit.....	175
HTTP keep-alive.....	176
skip scanning HTTP.....	176
trickling.....	176
external users.....	211
extranet devices	
configuring.....	30
<b>F</b>	
failover	
configuring on interface.....	141
firewall, definition.....	26
flow initial session timeout.....	127
forced timeout.....	112
fragmentation settings on WAP.....	384
fragmented packet size, maximum.....	127
FTP banner.....	164
FTP server, configuring on device.....	130
<b>G</b>	
G.lite.....	90
gateway tracking.....	305
GPRS	
configuring.....	131
GRE in TCP MSS option.....	128
GRE out TCP MSS option.....	128
GRE, configuring in device.....	62
group IKE ID.....	212
group, device.....	33
<b>H</b>	
HTTP banner.....	164
HTTP redirection.....	160
HTTP, configuring on device.....	159
hub-and-spoke policies for untrust MIP traffic,	
using.....	126
<b>I</b>	
ICMP path MTU discovery.....	123
Ident-Reset, enabling access on device	
interface.....	57
IGMP.....	336
IGMP proxy.....	337
import rules	
configuring on virtual router.....	300
integrated Web filtering, SurfControl (CPA).....	188
interface failover	
configuring on device.....	141
interfaces	
ADSL.....	88
advanced properties.....	55
aggregate.....	77
configuring for vsys.....	251

configuring on device.....	50	manual key.....	236
configuring WebAuth.....	55	messages	
general properties.....	53	configuring logging on device.....	167
loopback.....	79	email notification for device.....	167
protocol, configuring.....	61	MIB II.....	57
redundant.....	80	MIPs	
service options.....	56	configuring in device.....	62
subinterface.....	84	modem connection configuration.....	142
tunnel.....	87	modem settings, configuring on device.....	143
tunnel, MTU size.....	88	modules, Network and Security Manager.....	13
virtual security (VSI).....	80	multicast routing	
internal AV scanner		about.....	335
content drop parameters.....	177	IGMP.....	336
content protocol.....	178	negative mroute cache.....	344
pattern server URL.....	176	PIM-SM.....	339
update interval.....	177	routing table entries.....	344
ISP settings, configuring on device.....	143	multimedia sessions, SIP.....	279
ITU 992.2.....	90		
ITU G.992.1.....	90	<b>N</b>	
<b>J</b>		NACN, configuring on device.....	141
Job Manager		NAT objects.....	210
about.....	20	NAT, configuring on device.....	62
<b>L</b>		navigation tree.....	14
L2TP.....	233	negative mroute cache.....	344
local users.....	211	Network and Security Manager modules.....	13
log destinations		network modules	
configuring on device.....	167	about.....	396
log entries		chassis cards.....	399
configuring on device.....	167	copper I/O cards.....	397
Log Investigator		fiber I/O cards.....	397
about.....	15	secure port modules (SPM).....	398
log reason for session close.....	113	network options, configuring on device.....	34
log severity		Network Time Protocol (NTP).....	162
configuring on device.....	167	next-hop, configuring on virtual router.....	296
Log Viewer		NSGP	
about.....	14	about.....	131
loopback interface		enabling access on device interface.....	57
configuring.....	79	overbilling.....	131
<b>M</b>		NSM reporting, configuring on device.....	167
MAC access lists on WAP.....	387	NSM, enabling access on device interface.....	57
MAC flooding, allow unknown.....	124	NSRP	
main display area.....	14	synchronizing cluster configurations.....	370
management options for device administrators		NSRP clusters	
SSH.....	56	about.....	361
Telnet.....	56	active/active.....	368
Web UI.....	56	configuring cluster.....	362
		creating cluster.....	363
		DIP groups.....	100
		master/backup.....	371

- RTO mirror groups.....371
- RTOs.....371
- secure communications.....362
- synchronizing.....369
- VSD groups.....368
- VSI.....368
- NTP
  - configuring on device.....162
  - server, configuring on device.....162
- numbered tunnel interfaces.....87
- O**
- Object Manager
  - about.....18
- operation mode on WAP.....382
- OSPF
  - about.....311
  - configuring areas.....314
  - configuring authentication.....317
  - configuring interface link type.....316
  - configuring neighbors.....317
  - configuring parameters on virtual router.....313
  - configuring redistribution rules.....314
  - configuring summary import.....314
  - configuring tunnel interface as demand
    - circuit.....316
  - configuring virtual links.....315
  - enabling on device.....312
  - ignoring MTU mismatch in DB exchange.....316
  - not so stubby area (NSSA).....314
  - open shortest path first.....311
  - reduce LSA flooding.....316
  - stub area.....314
- overbilling.....131
- overlapping subnets, ignoring on virtual
  - router.....296
- P**
- packet flow, configuring on device.....122
- password length, restricting.....154
- passwords, device administrators.....150
- permitted IPs.....152
- PIM-SM
  - acceptable groups.....341
  - proxy rendezvous point.....342
  - rendezvous point to group mapping.....340
- ping, enabling access on device interface.....57
- pinholes.....287
- PKI defaults
  - configuring on device.....274
  - revocation settings.....275
  - SCEP.....275
- policy schedule.....114
- PPP.....90
- PPPoA
  - configuring on device.....141
  - using on ADSL interface.....90
- PPPoE
  - assigning to a VSI interface.....135
  - automatic update of DNS servers.....136
  - configuring on device.....135
  - multiple sessions on single interface.....138
- PPPoE, using on ADSL interface.....90
- preamble settings on WAP.....386
- predefined service timeouts, configuring on
  - device.....115
- priority levels for traffic shaping.....120
- protected resources.....209
- protocols
  - NSRP.....361
- public key authentication (PKA), device
  - administrators.....150
- R**
- reactivating settings on WAP.....394
- Realtime Monitor module.....15
- redundant interface.....80
- Report Manager module.....15
- reporting options on device
  - email notification.....167
  - messages and destinations.....167
  - SNMP.....167
  - syslog.....167
  - WebTrends.....168
- reset hardware (device).....155
- RIP
  - about.....319
  - alternate routes per prefix.....321
  - configure tunnel interface as demand
    - circuit.....324
  - configuring authentication.....324
  - configuring neighbors.....324
  - configuring parameters.....321
  - configuring redistribution rules.....323
  - configuring summary import.....323
  - enable summarization.....324
  - enabling.....320

hold down time.....	322	modules, Security Policies.....	17
poll interval for demand circuits.....	322	modules, Server Manager.....	20
retransmit interval for demand circuits.....	322	UI, about.....	12
split horizon.....	324	UI, main display area.....	14
timers.....	322	UI, navigation tree.....	14
version on interface.....	324	UI, status bar.....	14
version on virtual router instance.....	321	UI, toolbar.....	14
root device administrator.....	148	security policies	
route exporting.....	296	about.....	17
route lookup preference.....	295	serial link	
route maps		configuring ISP settings on device.....	143
about.....	298	configuring on device.....	142
offset metric.....	300	Server Manager module.....	20
preserve preference.....	299	service options	
setting match conditions.....	298	Ident-Reset.....	57
setting permitted route attributes.....	299	NSGP.....	57
route preferences, configuring on virtual		NSM.....	57
router.....	310	ping.....	57
routes, about.....	293	SNMP.....	57
Routing Information Protocol.....	319	SSH.....	56
routing table entries		SSL.....	57
configuring.....	303	Telnet.....	56
keep route active when interface is down.....	304	Web UI.....	56
metric.....	304	session close	
preference.....	304	log reason.....	113
RTOs		short slots on WAP.....	386
about.....	371	SIBR.....	307
mirror groups.....	371	SIP	
RTS/CTS settings.....	385	ALG.....	284
<b>S</b>		attack protection.....	117
SCEP.....	275	defined.....	279
SCP		destination IP server protection.....	117
using for SSH.....	156	incoming DIP for.....	73
searching in UI		INVITE messages.....	117
about.....	22	messages.....	279
secondary banner.....	158	multimedia sessions.....	279
secondary IP, configuring in device.....	61	request methods.....	280
secure copy.....	156	response codes.....	283
Security.....	173	signaling.....	284
Security Manager.....	17	SIP timeouts	
modules, Audit Log Viewer.....	16	inactivity.....	288
modules, Device Manager.....	16	media inactivity.....	288
modules, Job Manager.....	20	signaling inactivity.....	288
modules, Log Investigator.....	15	site survey.....	395
modules, Log Viewer.....	14	SMTP mail server, specifying on device.....	167
modules, Object Manager.....	18		
modules, Realtime Monitor.....	15		
modules, Report Manager.....	15		

SNMP	
configuring on device.....	167
enabling access on device interface.....	57
private traps, configuring on virtual router.....	296
split DNS queries, configuring on device.....	104
SSH	
configuring on device.....	156
enabling access on device interface.....	56
port, configuring for device CLI management.....	154
SSHv1, configuring on device.....	157
SSHv2, configuring on device.....	157
SSIDs on WAP.....	388
SSL	
configuring on device.....	160
disabling on device.....	161
enabling access on device interface.....	57
redirection.....	160
SSLHP.....	160
SSLHP.....	160
SSP	
using instead of TFTP.....	130
using to load certificates.....	271
using to load firmware.....	269
using to load PKA keys.....	150
status bar.....	14
subinterface.....	84
Super G.....	402
support, technical See technical support	
SurfControl	
Content Portal Authority (CPA).....	189
CPA (Integrated).....	189
synchronizing NSRP configurations.....	370
syslog reporting	
configuring on device.....	167
configuring syslog host.....	167
<b>T</b>	
TCP MSS option.....	127
TCP MSS, all option.....	127
TCP MSS, GRE in.....	128
TCP MSS, GRE out.....	128
TCP RST bit and sequence number, check.....	126
TCP RST invalid session.....	124
TCP sequence number check, skip.....	124
TCP SYN bit before create session for tunneled packets, check.....	125
TCP SYN bit before create session, check.....	125
technical support	
contacting JTAC.....	xviii
Telnet	
banner.....	164
enabling access on device interface.....	56
port, configuring for device CLI management.....	154
templates	
about.....	32
benefits.....	32
temporal key integrity protocol.....	393
TFTP/FTP server, configuring on device.....	130
time, setting on device.....	162
TKIP.....	393
toolbar in UI.....	14
traffic shaping	
configuring on device.....	119
DSCP class selector.....	120
mode.....	120
transmission power level settings on WAP.....	382
trustee privileges.....	148
tunnel interfaces	
about.....	87
configuring for VPN.....	213
MTU size.....	88
tunnel zones	
configuring.....	213
<b>U</b>	
unnumbered tunnel interfaces.....	87
<b>V</b>	
VIP options, configuring on device.....	108
VIPs	
configuring in device.....	65
mapping services and ports.....	65
virtual routers	
about.....	292, 359, 400
access lists.....	296
configuring for vsys.....	248
configuring on device.....	294
configuring RIP.....	319
consider active routes.....	296
destination-based routes.....	305
dynamic routing protocols.....	311
export and import rules.....	300
gateway tracking.....	305
general properties.....	295
ignore overlapping subnets.....	296

maximum equal cost routes.....	295	fragmentation.....	384
maximum number of routes.....	295	MAC access lists.....	387
multicast routing.....	335	operation mode.....	382
next-hop.....	296	preamble.....	386
route exporting.....	296	reactivating.....	394
route lookup preference.....	295	short slots.....	386
route maps.....	298	SSIDs.....	388
route preferences.....	310	transmission power level.....	382
routing table entries.....	303	WEP.....	390
shared VR.....	296	WEP keys.....	391
SNMP private traps.....	296	WPA.....	393
synchronizing/unsynchronizing.....	370	WPA rekey.....	393
virtual router ID.....	295	WPA-PSK passphrase.....	394
VoIP, configuring custom DHCP options for.....	59	WPA-PSK pre-shared key.....	394
VPN Manager.....	17, 194	WLAN	
expanded view.....	195	configurations, reactivating.....	402
VPNs.....	195, 196, 199, 200, 201, 204, 208, 209, 210, 211, 212, 217, 219, 229, 233, 235, 277, 291	configuring Super G.....	402
VSD groups.....	368	XR.....	402
VSIs.....	80, 368	WLAN settings.....	408
vsys		WPA rekey settings on WAP.....	393
about.....	248	WPA settings on WAP.....	393
administrators.....	149	WPA-PSK	
configuring interfaces.....	251	passphrase settings on WAP.....	394
configuring virtual routers.....	248	pre shared key on WAP.....	394
configuring zones.....	249	settings on WAP.....	393
limitations.....	354	WPA2, XR, and SuperG.....	399
per CPU limit.....	357		
per session limit.....	356	X	
read-only admins.....	149	X509 certificates.....	274
viewing configuration.....	252	XR, configuring.....	402
W		Z	
Web management, configuring on device.....	159	zone	
Web UI, enabling access on device interface.....	56	adding on device.....	39
WebAuth		configuring for vsys.....	249
banners.....	164	configuring on device.....	39
WebTrends			
reporting, configuring on device.....	168		
WEP keys on WAP.....	391		
WEP settings on WAP.....	390		
wireless settings			
about.....	408		
aging.....	383		
antenna.....	381		
beacon.....	384		
burst.....	384		
channel.....	381		
control frame protection.....	385		
data rate.....	383		