



---

Junos<sup>®</sup> Space

Security Design User Guide

Release  
12.1



---

Published: 2012-05-22

Juniper Networks, Inc.  
1194 North Mathilda Avenue  
Sunnyvale, California 94089  
408-745-2000  
www.juniper.net

This product includes the Envoy SNMP Engine, developed by Epilogue Technology, an Integrated Systems Company. Copyright © 1986-1997, Epilogue Technology Corporation. All rights reserved. This program and its documentation were developed at private expense, and no part of them is in the public domain.

This product includes memory allocation software developed by Mark Moraes, copyright © 1988, 1989, 1993, University of Toronto.

This product includes FreeBSD software developed by the University of California, Berkeley, and its contributors. All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by the Regents of the University of California. Copyright © 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994. The Regents of the University of California. All rights reserved.

GateD software copyright © 1995, the Regents of the University. All rights reserved. Gate Daemon was originated and developed through release 3.0 by Cornell University and its collaborators. Gated is based on Kirton's EGP, UC Berkeley's routing daemon (routed), and DCN's HELLO routing protocol. Development of Gated has been supported in part by the National Science Foundation. Portions of the GateD software copyright © 1988, Regents of the University of California. All rights reserved. Portions of the GateD software copyright © 1991, D. L. S. Associates.

This product includes software developed by Maker Communications, Inc., copyright © 1996, 1997, Maker Communications, Inc.

Juniper Networks, the Juniper Networks logo, JUNOS, NetScreen, ScreenOS, and Steel-Belted Radius are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOSe is a trademark 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.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

*Junos Space Security Design User Guide*  
Copyright © 2011, Juniper Networks, Inc.  
All rights reserved. Printed in USA.

Revision History  
May 2012—Junos Space Security Design User Guide, Release 12.1

The information in this document is current as of the date listed in the revision history.

#### YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. The Junos OS has no known time-related limitations through the 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

	About This Guide . . . . .	xv
	Junos Space Documentation and Release Notes . . . . .	xv
	Documentation Conventions . . . . .	xv
	Documentation Feedback . . . . .	xvi
	Requesting Technical Support . . . . .	xvi
	Self-Help Online Tools and Resources . . . . .	xvi
	Opening a Case with JTAC . . . . .	xvii
<b>Part 1</b>	<b>Security Design Overview</b>	
<b>Chapter 1</b>	<b>Security Design Overview . . . . .</b>	<b>3</b>
	Security Design Overview . . . . .	3
<b>Chapter 2</b>	<b>Security Design Dashboard . . . . .</b>	<b>7</b>
	Security Design Dashboard . . . . .	7
<b>Part 2</b>	<b>Getting Started</b>	
<b>Chapter 3</b>	<b>Getting Started with Security Design . . . . .</b>	<b>13</b>
	Getting Started . . . . .	13
	Provisioning Firewall Policies . . . . .	13
	Provisioning NAT Policies . . . . .	13
	Provisioning IPsec VPNs . . . . .	14
	IPS Management . . . . .	14
	AppFW Management . . . . .	14
<b>Part 3</b>	<b>Object Builder</b>	
<b>Chapter 4</b>	<b>Object Builder Overview . . . . .</b>	<b>19</b>
	Object Builder Overview . . . . .	19
<b>Chapter 5</b>	<b>Service and Service Groups . . . . .</b>	<b>21</b>
	Service and Service Group Overview . . . . .	21
	Creating Services . . . . .	22
	Managing Services . . . . .	25
	Modifying a Service . . . . .	25
	Deleting a Service . . . . .	26

	Cloning a Service . . . . .	26
	Find Duplicate Service Objects . . . . .	26
	Creating Service Groups . . . . .	27
	Managing Service Groups . . . . .	28
	Modifying a Service Group . . . . .	29
	Deleting a Service Group . . . . .	29
	Cloning a Service Group . . . . .	29
<b>Chapter 6</b>	<b>Addresses and Address Groups . . . . .</b>	<b>31</b>
	Address and Address Groups Overview . . . . .	31
	Creating Addresses . . . . .	31
	Managing Addresses . . . . .	33
	Modifying an Address . . . . .	34
	Deleting an Address . . . . .	34
	Cloning an Address . . . . .	34
	Exporting Addresses . . . . .	35
	Importing Addresses . . . . .	35
	Find Duplicate Address Objects . . . . .	35
	Creating Address Groups . . . . .	38
	Managing Address Groups . . . . .	39
	Modifying an Address Group . . . . .	39
	Deleting an Address Group . . . . .	39
	Cloning an Address Group . . . . .	40
<b>Chapter 7</b>	<b>Extranet Devices . . . . .</b>	<b>41</b>
	Creating Extranet Devices . . . . .	41
	Managing Extranet Devices . . . . .	42
	Modifying an Extranet Device . . . . .	42
	Deleting an Extranet Device . . . . .	42
	Cloning an Extranet Device . . . . .	43
<b>Chapter 8</b>	<b>Application Signatures . . . . .</b>	<b>45</b>
	Creating Application Signatures . . . . .	45
	Managing Application Signatures . . . . .	47
	Filtering Application Signatures . . . . .	47
	Modifying Application Signatures . . . . .	48
	Deleting Application Signatures . . . . .	48
	Cloning Application Signatures . . . . .	48
	Creating an Application Signature Group . . . . .	49
<b>Chapter 9</b>	<b>NAT Pools . . . . .</b>	<b>51</b>
	Creating NAT Pools . . . . .	52
	Managing NAT Pools . . . . .	53
	Deleting NAT Pools . . . . .	53
	Modifying NAT Pools . . . . .	54
	Cloning NAT Pools . . . . .	54

<b>Chapter 10</b>	<b>Policy Profiles</b> .....	<b>57</b>
	Security Policy Profiles Overview .....	57
	Creating Policy Profiles .....	58
	Managing Policy Profiles .....	60
	Deleting Policy Profiles .....	61
	Modifying Policy Profiles .....	61
	Cloning Policy Profiles .....	61
<b>Chapter 11</b>	<b>VPN Profiles</b> .....	<b>63</b>
	VPN Profiles Overview .....	63
	Creating VPN Profiles .....	63
	Managing VPN Profiles .....	66
	Deleting VPN Profiles .....	66
	Modifying VPN Profiles .....	67
	Cloning VPN Profiles .....	67
<b>Chapter 12</b>	<b>Variables</b> .....	<b>69</b>
	Creating Variable Definitions .....	69
	Managing Variable Definitions .....	71
	Deleting Variable Definitions .....	71
	Modifying Variable Definitions .....	72
	Cloning Variable Definitions .....	72
<b>Chapter 13</b>	<b>Template Definitions</b> .....	<b>73</b>
	Creating Template Definitions .....	73
	Managing Template Definitions .....	74
	Deleting Template Definitions .....	74
	Modifying Template Definitions .....	75
<b>Chapter 14</b>	<b>Templates</b> .....	<b>77</b>
	Creating Templates .....	77
	Managing Templates .....	78
	Deleting Templates .....	78
	Modifying Templates .....	79
<b>Part 4</b>	<b>Firewall Policy</b>	
<b>Chapter 15</b>	<b>Firewall Policy</b> .....	<b>83</b>
	Firewall Policies Overview .....	83
	Rule Base Overview .....	84
	Example: UnManaging a Previously Managed Rule Base .....	85
	Multiple Group Policy Membership Overview .....	85
	General Rules About Priority and Precedence .....	86
	Example: New Precedence of a Policy Set to the Same Precedence as an Existing Policy .....	86
	Sorting of Firewall Policy Left Pane .....	86
	Global Address Book Overview .....	87
	Differences Between Global and Zone-Based Address Books .....	88
	Nested Address Group Support .....	88
	Mixed-Version Support .....	88

	Migrating from Zone to Global Addressing . . . . .	89
	Creating Firewall Policies . . . . .	90
	Inline Creation of Objects in Policy . . . . .	98
	Policy Priority Precedence Setting . . . . .	103
	Adding Rules to a Firewall Policy . . . . .	107
	Ordering the Rules in a Firewall Policy . . . . .	110
	Publishing Firewall Policies . . . . .	111
	Custom Columns in Firewall Policy . . . . .	117
	Custom Column Overview . . . . .	117
	Creating Custom Column Definitions . . . . .	117
	Custom Column Data Search . . . . .	118
	Managing Custom Column Definitions . . . . .	119
	Managing Custom Column Data . . . . .	119
	Modifying Custom Columns Definitions . . . . .	120
	Deleting a Custom Columns Definition . . . . .	120
	Exporting a Custom Columns Definition . . . . .	121
	Managing Firewall Policies . . . . .	121
	Modifying Firewall Policies . . . . .	121
	Deleting Firewall Policies . . . . .	122
	Cloning Firewall Policies . . . . .	123
	Promoting a Firewall Policy . . . . .	124
	Exporting a Firewall Policy . . . . .	124
	Deleting Rules in a Firewall Policy . . . . .	125
	Cloning a Rule in a Firewall Policy . . . . .	125
	Grouping Rules in a Firewall Policy . . . . .	125
	Enabling/Disabling Rules in a Firewall Policy . . . . .	126
	Copying And Pasting Rules in Firewall Policy . . . . .	126
	Assigning Devices to a Firewall Policy . . . . .	127
	Deleting Devices from a Firewall Policy . . . . .	127
<b>Part 5</b>	<b>VPN</b>	
<b>Chapter 16</b>	<b>VPN . . . . .</b>	<b>131</b>
	IPsec VPN Overview . . . . .	131
	Creating IPsec VPNs . . . . .	132
	Creating IPsec VPNs . . . . .	133
	Publishing IPsec VPNs . . . . .	141
	Managing IPsec VPNs . . . . .	143
	Modifying IPsec VPNs . . . . .	143
	Modifying Endpoint Settings in a VPN . . . . .	144
	Deleting IPsec VPNs . . . . .	145
<b>Part 6</b>	<b>NAT Policies</b>	
<b>Chapter 17</b>	<b>NAT Policy . . . . .</b>	<b>149</b>
	NAT Overview . . . . .	149
	Creating NAT Policies . . . . .	151
	Adding Rules to a NAT Policy . . . . .	156
	Ordering the Rules in a NAT Policy . . . . .	160

	Publishing NAT Policies . . . . .	161
	Managing NAT Policies . . . . .	163
	Modifying NAT Policies . . . . .	163
	Deleting NAT Policies . . . . .	163
	Cloning NAT Policies . . . . .	164
	Exporting a NAT Policy . . . . .	164
	Deleting Rules in a NAT Policy . . . . .	164
	Grouping Rules in a NAT Policy . . . . .	165
	Enabling/Disabling Rules in a NAT Policy . . . . .	165
	Copying and Pasting Rules in a NAT Policy . . . . .	166
	Assigning Devices to a NAT Policy . . . . .	167
	Deleting Devices from a NAT Policy . . . . .	167
<b>Part 7</b>	<b>Global Search</b>	
<b>Chapter 18</b>	<b>Global Search . . . . .</b>	<b>171</b>
	Global Search . . . . .	171
<b>Part 8</b>	<b>Downloads</b>	
<b>Chapter 19</b>	<b>Downloads . . . . .</b>	<b>175</b>
	Downloading the Signature Database . . . . .	175
	Installing the Signature Database . . . . .	177
<b>Part 9</b>	<b>IPS Management</b>	
<b>Chapter 20</b>	<b>IPS Management Overview . . . . .</b>	<b>183</b>
	IPS Management Overview . . . . .	183
<b>Chapter 21</b>	<b>IPS Management . . . . .</b>	<b>185</b>
	Creating IPS Signatures . . . . .	185
	Managing IPS Signatures . . . . .	187
	Filtering IPS Signatures . . . . .	188
	Modifying IPS Signatures . . . . .	188
	Deleting IPS Signatures . . . . .	188
	Cloning IPS Signatures . . . . .	189
	Creating Static Signature Groups . . . . .	189
	Creating Dynamic Signature Groups . . . . .	190
	Creating IPS Signature-sets . . . . .	190
	Creating IPS Signature Sets . . . . .	191
	Adding Rules to an IPS Signature Set . . . . .	192
	Managing IPS Signature Sets . . . . .	193
	Deleting IPS Signature-sets . . . . .	193
	Cloning IPS Signature-sets . . . . .	193
	Enable or Disable Rules in an IPS Signature-set . . . . .	194
	Creating IPS Policies . . . . .	195
	Publishing IPS Policies . . . . .	198
	Managing IPS Policies . . . . .	201
	Deleting IPS Policy Rules . . . . .	201
	Enabling or Disabling Rules in an IPS Policy . . . . .	201

<b>Part 10</b>	<b>Security Design Devices</b>	
<b>Chapter 22</b>	<b>Security Design Devices</b>	<b>205</b>
	Updating Devices with Pending Services	205
	Importing Firewall and NAT Policies from a Device to Security Design	207
	NSM Migration	211
<b>Part 11</b>	<b>Index</b>	
	Index	219



# List of Figures

<b>Part 1</b>	<b>Security Design Overview</b>	
<b>Chapter 1</b>	<b>Security Design Overview</b>	<b>3</b>
	Figure 1: Security Design Home Page	4
<b>Chapter 2</b>	<b>Security Design Dashboard</b>	<b>7</b>
	Figure 2: Object Count Gadget	9
	Figure 3: Address Types Gadgets	9
<b>Part 3</b>	<b>Object Builder</b>	
<b>Chapter 5</b>	<b>Service and Service Groups</b>	<b>21</b>
	Figure 4: Create Service: Basic View Page	22
	Figure 5: Create Service: Advanced Settings Page	23
	Figure 6: Create Service Group Page	28
<b>Chapter 6</b>	<b>Addresses and Address Groups</b>	<b>31</b>
	Figure 7: Create Address Page	32
	Figure 8: Page Showing Duplicate Address Objects	36
	Figure 9: Merge Address Page	36
	Figure 10: Merge Operation Confirmation Message	36
	Figure 11: Duplicate Objects Delete Confirmation Page	37
	Figure 12: Duplicate Objects Usage Window	37
	Figure 13: Create Address Group Page	38
<b>Chapter 7</b>	<b>Extranet Devices</b>	<b>41</b>
	Figure 14: Create Extranet Device Page	41
<b>Chapter 8</b>	<b>Application Signatures</b>	<b>45</b>
	Figure 15: Application Signatures Page	45
	Figure 16: Create Application Signature Page	46
<b>Chapter 9</b>	<b>NAT Pools</b>	<b>51</b>
	Figure 17: Create NAT Pool Page	52
<b>Chapter 10</b>	<b>Policy Profiles</b>	<b>57</b>
	Figure 18: New Policy Profile Page	59
<b>Chapter 11</b>	<b>VPN Profiles</b>	<b>63</b>
	Figure 19: VPN Profile: Phase 1	64
	Figure 20: VPN Profile: Phase 2	65
<b>Chapter 12</b>	<b>Variables</b>	<b>69</b>
	Figure 21: Create Polymorphic Object Page	70

<b>Chapter 13</b>	<b>Template Definitions . . . . .</b>	<b>73</b>
	Figure 22: Create Template Definition Page . . . . .	74
<b>Chapter 14</b>	<b>Templates . . . . .</b>	<b>77</b>
	Figure 23: Create Template Page . . . . .	78
<b>Part 4</b>	<b>Firewall Policy</b>	
<b>Chapter 15</b>	<b>Firewall Policy . . . . .</b>	<b>83</b>
	Figure 24: Sorting Order in the Firewall Policy Left Pane . . . . .	86
	Figure 25: Firewall Policy Tabular View . . . . .	91
	Figure 26: Tooltip Showing Object Information . . . . .	93
	Figure 27: Create Firewall Policy . . . . .	94
	Figure 28: Turning an IPS Policy on or off . . . . .	95
	Figure 29: Source Identity Page . . . . .	97
	Figure 30: Select Devices Page . . . . .	98
	Figure 31: Inline Address Object Creation in the Source Address Window . . . . .	99
	Figure 32: Inline Address Object Create Page . . . . .	99
	Figure 33: Address Selector Page Showing the New Inline Object . . . . .	100
	Figure 34: Inline Service Object Creation in the Service List . . . . .	101
	Figure 35: Inline Service Object Creation Page . . . . .	101
	Figure 36: Service Selector Page Showing the New Object . . . . .	102
	Figure 37: Policy: Priority And Precedence Page . . . . .	104
	Figure 38: Priority Precedence Tool Tip . . . . .	104
	Figure 39: Priority And Precedence Right-Click Page . . . . .	106
	Figure 40: Setting Priority And Precedence Value Page . . . . .	106
	Figure 41: Tunnel Option for Global Rule . . . . .	108
	Figure 42: Concurrent Policy Edit Error Message . . . . .	110
	Figure 43: Policy Publish Page . . . . .	112
	Figure 44: Devices on Which the Policies Will Be Published . . . . .	113
	Figure 45: Policy Publish: CLI Configuration . . . . .	113
	Figure 46: Device Validation Warning Message . . . . .	114
	Figure 47: Policy Publish: LSYS Device CLI Configuration . . . . .	114
	Figure 48: Policy Publish: XML Configuration . . . . .	115
	Figure 49: Creating Custom Column . . . . .	117
	Figure 50: Creating Custom Column Page . . . . .	118
	Figure 51: Create Custom Column Confirm Page . . . . .	118
	Figure 52: Custom Column Data Search . . . . .	119
	Figure 53: Modifying a Custom Column . . . . .	120
	Figure 54: Deleting a Custom Column . . . . .	120
	Figure 55: Modify Policy Page . . . . .	122
	Figure 56: Clone Policy Page . . . . .	123
	Figure 57: Promote Policy Page . . . . .	124
	Figure 58: Variable Objects Rule Paste Error . . . . .	127
<b>Part 5</b>	<b>VPN</b>	
<b>Chapter 16</b>	<b>VPN . . . . .</b>	<b>131</b>
	Figure 59: VPN Landing Page . . . . .	133
	Figure 60: Create VPN Page—Route-Based VPN . . . . .	134

	Figure 61: Create VPN: Add as Endpoint Page . . . . .	135
	Figure 62: Create VPN—Tunnel, Route, and Global Setting Pane . . . . .	136
	Figure 63: Create VPN Page Showing Custom Routing Instance Option . . . . .	137
	Figure 64: Create VPN—Route-Based VPN Preview . . . . .	138
	Figure 65: Create VPN Policy-Based—Add as Endpoint Page . . . . .	139
	Figure 66: Create VPN Page—External Interface Selection . . . . .	140
	Figure 67: Inline Address Object Creation Page . . . . .	141
<b>Part 6</b>	<b>NAT Policies</b>	
<b>Chapter 17</b>	<b>NAT Policy . . . . .</b>	<b>149</b>
	Figure 68: NAT Policy Tabular View . . . . .	151
	Figure 69: Create NAT Policy Page . . . . .	152
	Figure 70: Setting Source NAT Pool Page . . . . .	153
	Figure 71: Create Source NAT Pool Page . . . . .	153
	Figure 72: Setting the Destination Pool Page . . . . .	154
	Figure 73: Create Destination NAT Pool Page . . . . .	154
	Figure 74: Create Inline NAT Address Object . . . . .	154
	Figure 75: Create NAT Address Page . . . . .	155
	Figure 76: Destination Traffic Match Type Selector Page . . . . .	157
	Figure 77: Routing Instance Selection Page . . . . .	158
	Figure 78: Concurrent NAT Policy Editing Error . . . . .	160
	Figure 79: NAT Policy CLI Configuration . . . . .	162
	Figure 80: Rule Copy Paste Options . . . . .	166
	Figure 81: Destination NAT Rule Paste Error . . . . .	166
	Figure 82: Static NAT Rule Paste Error . . . . .	167
	Figure 83: Group Policy Paste Error . . . . .	167
<b>Part 7</b>	<b>Global Search</b>	
<b>Chapter 18</b>	<b>Global Search . . . . .</b>	<b>171</b>
	Figure 84: Global Search Results . . . . .	171
<b>Part 8</b>	<b>Downloads</b>	
<b>Chapter 19</b>	<b>Downloads . . . . .</b>	<b>175</b>
	Figure 85: Signature Download Logs . . . . .	175
	Figure 86: Signature Database Page . . . . .	176
	Figure 87: Download Configuration Page . . . . .	176
	Figure 88: Install Configuration Page . . . . .	178
<b>Part 9</b>	<b>IPS Management</b>	
<b>Chapter 21</b>	<b>IPS Management . . . . .</b>	<b>185</b>
	Figure 89: View All IPS Signatures Page . . . . .	186
	Figure 90: Create IPS Signature Page . . . . .	186
	Figure 91: IPS Signature Set Tabular View . . . . .	191
	Figure 92: IPS Management Right Pane View . . . . .	195
	Figure 93: IPS Policies Tabular View . . . . .	196
	Figure 94: Create IPS Policy Address Objects Page . . . . .	197

Figure 95: Create IPS Policy Address Page . . . . .	197
Figure 96: IPS Policy Publish Page . . . . .	198
Figure 97: Policy Publish: Affected Devices Page . . . . .	199
Figure 98: Policy Publish: CLI Configuration . . . . .	199
Figure 99: Policy Publish: XML Configuration . . . . .	200

## Part 10

### Chapter 22

## Security Design Devices

<b>Security Design Devices . . . . .</b>	<b>205</b>
Figure 100: Security Design Devices Page . . . . .	205
Figure 101: Update Window . . . . .	206
Figure 102: Device Changes Page Showing Device Comments . . . . .	206
Figure 103: Manage Security Devices Page . . . . .	207
Figure 104: Service Import Summary Page . . . . .	208
Figure 105: Object Conflict Resolution Page for Firewall Policy . . . . .	208
Figure 106: Firewall Policy Import Status Page . . . . .	209
Figure 107: Firewall Policy Final Import Status Page . . . . .	210
Figure 108: High-level Device Import Workflow . . . . .	212
Figure 109: NSM Xdiff File Upload Page . . . . .	212
Figure 110: NSM Migration Devices Page . . . . .	213
Figure 111: Service Import Summary Page . . . . .	213
Figure 112: NSM—Object Conflict Resolution Page . . . . .	214
Figure 113: NSM Migration Status Page . . . . .	214
Figure 114: NSM Migration Final Status Report Page . . . . .	215

# List of Tables

	<b>About This Guide</b> . . . . .	<b>xv</b>
	Table 1: Notice Icons . . . . .	xv
<b>Part 1</b>	<b>Security Design Overview</b>	
<b>Chapter 2</b>	<b>Security Design Dashboard</b> . . . . .	<b>7</b>
	Table 2: Security Design Workspaces . . . . .	8
<b>Part 4</b>	<b>Firewall Policy</b>	
<b>Chapter 15</b>	<b>Firewall Policy</b> . . . . .	<b>83</b>
	Table 3: Sorting Order for Firewall Policies . . . . .	86
	Table 4: Migration Matrix . . . . .	89
	Table 5: Firewall policy Right Page Search Options . . . . .	91
	Table 6: IPS Configuration Mode . . . . .	95
	Table 7: Priority and Precedence for Firewall Policies . . . . .	105
	Table 8: IPS Field Options . . . . .	109
	Table 9: Setting Precedence Values for Different Priorities . . . . .	122
<b>Part 7</b>	<b>Global Search</b>	
<b>Chapter 18</b>	<b>Global Search</b> . . . . .	<b>171</b>
	Table 10: Security Design Global Search . . . . .	171



# About This Guide

- [Junos Space Documentation and Release Notes on page xv](#)
- [Documentation Conventions on page xv](#)
- [Documentation Feedback on page xvi](#)
- [Requesting Technical Support on page xvi](#)

## Junos Space Documentation and Release Notes

---

For a list of related Junos Space documentation, see <http://www.juniper.net/techpubs/>.

If the information in the latest release notes differs from the information in the documentation, follow the *Junos Space Release Notes*.




To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at <http://www.juniper.net/techpubs/>.

## Documentation Conventions

---

[Table 1 on page xv](#) defines notice icons used in this documentation.

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.

## Documentation Feedback

---

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to [techpubs-comments@juniper.net](mailto:techpubs-comments@juniper.net), or fill out the documentation feedback form at <https://www.juniper.net/cgi-bin/docbugreport/>. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

## 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 post-sales 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 Management tool: <http://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <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 Management 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, see <http://www.juniper.net/support/requesting-support.html> .



## PART 1

# Security Design Overview

- [Security Design Overview on page 3](#)
- [Security Design Dashboard on page 7](#)



## CHAPTER 1

# Security Design Overview

- [Security Design Overview on page 3](#)

## Security Design Overview

---

Security Design is a Junos Space application that you can use to design your network security using a quick and easy approach. With Security Design, you can create IPsec VPNs, firewall policies, NAT policies, and IPS configurations and push them to your security devices. These configurations use objects such as addresses, services, NAT pools, application signatures, policy profiles, VPN profiles, template definitions, and templates. These objects can be shared across multiple security configurations. You can create these objects prior to creating security configurations.

Firewall policy, NAT policy, and IPS policy can be created and managed in Tabular view. You can easily add new rules to the policies and choose to override policy-inherited settings by customizing the settings at a per-rule level. After you have added the rules to the policy, you can reorder these rules based on priority or group these rules for easy identification, and modify them at a later point in time. A unified user interface approach for firewall, NAT, and IPS policies helps you reduce the learning time required to create different security configurations.

Security Design allows you to create site-to-site, hub-and-spoke, and full mesh IPsec VPNs. The IPsec VPN creation interface allows you to define the Phase 1 and Phase 2 settings of the VPN. All VPNs created using Security Design can be viewed in Tabular view. You can also modify the settings at a per-VPN level or per-device level in a VPN.

You can periodically download the latest version of application signatures and IPS signatures from a URL provided by Juniper Networks. You can install these signatures on security devices that have an IPS-related license installed. You can then use application signatures and IPS signatures when creating firewall policy configurations. Security Design also lets you create your own customized signature-sets. All application firewall and IPS configurations are pushed to the devices when the firewall policy in which they are used is pushed to the devices.

When you finish creating and verifying your security configurations, you can publish these configurations and keep them ready to be pushed to the security devices. Security Design helps you push all the security configurations to the devices all at once by providing a single interface that is intuitive. You can select all security devices that you are using on the network and push all security configurations to these devices.

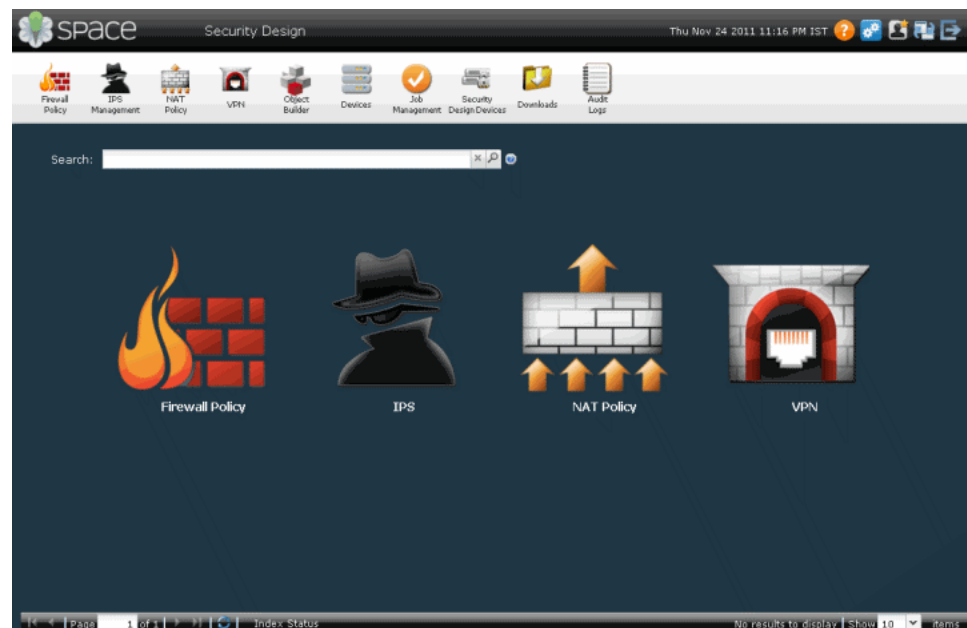
A set of gadgets displayed on the dashboard graphically illustrates the critical elements related to your security configurations. These gadgets help you keep track of the objects created and their usage across security configurations.

The Security Design application is divided into seven workspaces, which include Object Builder, Firewall Policy, NAT Policy, VPN, Downloads, IPS Management, and Security Design Devices.

- Object Builder - A workspace to create objects used for firewall policy, NAT policy and VPN configurations.
- Firewall Policy - A workspace to create and publish firewall policies on supported devices.
- NAT Policy - A workspace to create and publish NAT policies on supported devices.
- VPN - A workspace to create Hub And Spoke, Site to Site, and Full Mesh IPsec VPNs.
- Downloads - A workspace to download and install signatures.
- IPS Management - A workspace to create and manage IPS signatures, signature-sets, and IPS policies.
- Security Design Devices - A workspace to update the configurations on the devices.

Figure 1 on page 4 displays Security Design home page.

Figure 1: Security Design Home Page



Some of the global features available with Security Design include:

- Create unique labels for objects and security configurations using the Tagging feature for easier identification.
- Search objects and security configurations from a single search interface.

- Verify and tweak your security configurations before pushing them to the device by viewing the CLI and XML version of the configuration in the Publish workflow. This helps you keep the configurations ready and push these configurations to the devices during the maintenance window.
- Quickly clone objects and policy-related security configurations to save time and effort in creating new objects and configurations.





## CHAPTER 2

# Security Design Dashboard










- [Security Design Dashboard on page 7](#)

### Security Design Dashboard

---

[Table 2 on page 8](#) lists the workspaces on the Security Design dashboard.

Table 2: Security Design Workspaces

Icons	Workspace Name	Tasks
	Firewall Policy	Create, manage, and publish firewall policies.
	IPS Management	Create and manage IPS signatures, IPS signature-sets, and IPS policies.
	NAT Policy	Create, manage, and publish NAT policies.
	VPN	Create, manage, and publish VPNs.
	Object Builder	Create, modify, delete, and clone addresses, services, policy profiles, VPN profiles, application signatures, templates, template definitions, templates, and NAT pools.
	Devices	Manage, discover, and add devices.
	Job Management	Manage and view job status.
	Security Design Devices	Update the devices with firewall policies, NAT policies, and VPN configurations.
	Downloads	Download AppFirewall and IPS signatures.
	Audit Logs	View audit logs by task, user, workspace, and application.

The Security Design dashboard has gadgets with information that is updated automatically and immediately. You can move gadgets on the dashboard and resize them. These changes persist when you log out and log in to the Security Design application. The gadgets displayed on the Security Design dashboard are:

[Figure 2 on page 9](#) the Object Count gadget. This gadget shows the number of objects that are created from the Object Builder workspace. You can use this gadget to keep track of the objects available to create a security topology, IPsec VPNs, or security policies.

Figure 2: Object Count Gadget

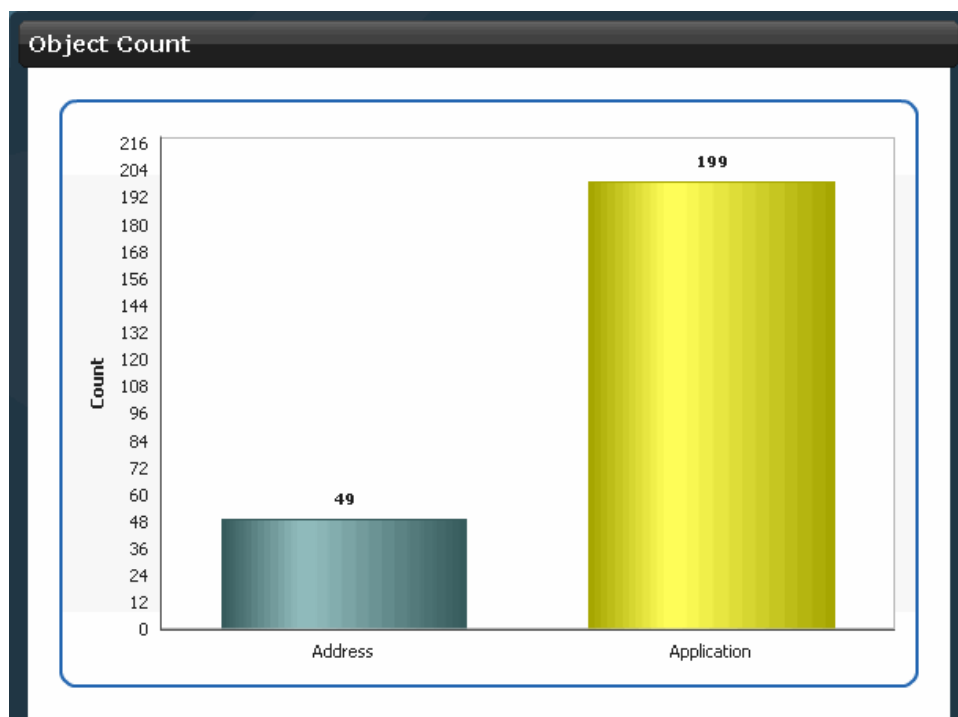
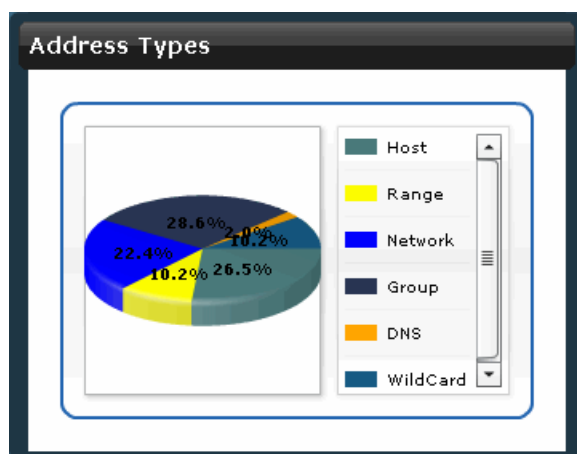


Figure 3 on page 9 shows the Address Types gadget. This gadget shows the different address types created using the Address Creation Wizard.

Figure 3: Address Types Gadgets





## PART 2

# Getting Started

- [Getting Started with Security Design on page 13](#)



## CHAPTER 3

# Getting Started with Security Design

- [Getting Started on page 13](#)

## Getting Started

---

The Getting Started assistant provides instructions on how to perform tasks related to a firewall policy, a NAT policy, a VPN, an IPS configuration, and an AppFirewall configuration in Security Design.

The **Getting Started** section displays instructions on how to:

1. [Provisioning Firewall Policies on page 13](#)
2. [Provisioning NAT Policies on page 13](#)
3. [Provisioning IPsec VPNs on page 14](#)
4. [IPS Management on page 14](#)
5. [AppFW Management on page 14](#)

## Provisioning Firewall Policies

To provision firewall policies:

1. Discover devices. See *Discovering Devices* section in the *Junos Space Network Application Platform User Guide*.
2. Create addresses. See [“Creating Addresses” on page 31](#).
3. Create a policy profile. See [“Creating Policy Profiles” on page 58](#).
4. Create a service. See [“Creating Services” on page 22](#).
5. Create firewall policies. See [“Creating Firewall Policies” on page 90](#).
6. Publish firewall policies. See [“Publishing Firewall Policies” on page 111](#)
7. Update devices. See [“Updating Devices with Pending Services” on page 205](#).

## Provisioning NAT Policies

To provision NAT policies:

1. Discover devices. See [Discovering Devices](#) section in the *Junos Space Network Application Platform User Guide*.
2. Create addresses. See [“Creating Addresses”](#) on page 31.
3. Create firewall policies. See [“Creating Firewall Policies”](#) on page 90.
4. Publish firewall policies. See [“Publishing Firewall Policies”](#) on page 111
5. Create NAT pools. See [“Creating NAT Pools”](#) on page 52
6. Create NAT policies. See [“Creating NAT Policies”](#) on page 151.
7. Publishing NAT policies. See [“Publishing NAT Policies”](#) on page 161
8. Update devices. See [“Updating Devices with Pending Services”](#) on page 205.

## Provisioning IPsec VPNs

To provision IPsec VPNs:

1. Discover devices. See [Discovering Devices](#) section in the *Junos Space Network Application Platform User Guide*.
2. Create addresses. See [“Creating Addresses”](#) on page 31.
3. Create a VPN profile. See [“Creating VPN Profiles”](#) on page 63.
4. Create an IPsec VPN. See [“Creating IPsec VPNs”](#) on page 132.
5. Publish the IPsec VPN. See [“Publishing IPsec VPNs”](#) on page 141.
6. Update devices. See [“Updating Devices with Pending Services”](#) on page 205.

## IPS Management

To manage IPS:

1. Discover devices. See [Discovering Devices](#) section in the *Junos Space Network Application Platform User Guide*.
2. Download IPS signature. See [“Downloading the Signature Database”](#) on page 175.
3. Pushing IPS signature to the device. See [“Installing the Signature Database”](#) on page 177.
4. Create a firewall policy with IPS enabled. See [“Creating Firewall Policies”](#) on page 90.
5. Publish firewall policies. See [“Publishing Firewall Policies”](#) on page 111.
6. Update devices. See [“Updating Devices with Pending Services”](#) on page 205.
7. Create IPS signature. See [“Creating IPS Signatures”](#) on page 185.
8. Create IPS signature-set. See [“Creating IPS Signature Sets”](#) on page 191.
9. Create IPS policies. See [“Creating IPS Policies”](#) on page 195.

## AppFW Management

To manage AppFW:



1. Discover devices. See Discovering Devices section in the *Junos Space Network Application Platform User Guide*.
2. Download application signature. See [“Downloading the Signature Database” on page 175](#).
3. Push application signature to the device. See [“Installing the Signature Database” on page 177](#).
4. Create a firewall policy with AppFW enabled. See [“Creating Firewall Policies” on page 90](#).
5. Publish firewall policies. See [“Publishing Firewall Policies” on page 111](#).
6. Update devices. See [“Updating Devices with Pending Services” on page 205](#).
7. Create application signature. See [“Creating Application Signatures” on page 45](#).



## PART 3

# Object Builder

- [Object Builder Overview on page 19](#)
- [Service and Service Groups on page 21](#)
- [Addresses and Address Groups on page 31](#)
- [Extranet Devices on page 41](#)
- [Application Signatures on page 45](#)
- [NAT Pools on page 51](#)
- [Policy Profiles on page 57](#)
- [VPN Profiles on page 63](#)
- [Variables on page 69](#)
- [Template Definitions on page 73](#)
- [Templates on page 77](#)



## CHAPTER 4

# Object Builder Overview

- [Object Builder Overview on page 19](#)

## Object Builder Overview

---

You can use the Object Builder workspace in Security Design to create objects used by firewall policies, VPNs, and NAT policies. These objects are stored in the Junos Space database. You can reuse these objects with multiple security policies, VPNs, and NAT policies. This makes the design of services more structured and avoids the need to create the objects during the service design.

You can use the Object Builder workspace to create, modify, clone, and delete the following objects:

- Addresses and address groups
- Services and service groups
- Application signatures
- Extranet devices
- NAT Pools
- Policy Profiles
- VPN Profiles
- Variables
- Template and template definitions

You will not be able to delete any of the objects you have created in Object Builder (except Template definition and Templates) if they are already used in one of the firewall policies, NAT policies, or VPNs.

### Related Documentation

- [Address and Address Groups Overview on page 31](#)
- [Service and Service Group Overview on page 21](#)
- [Security Policy Profiles Overview on page 57](#)
- [VPN Profiles Overview on page 63](#)



## CHAPTER 5

# Service and Service Groups

- [Service and Service Group Overview on page 21](#)
- [Creating Services on page 22](#)
- [Managing Services on page 25](#)
- [Creating Service Groups on page 27](#)
- [Managing Service Groups on page 28](#)

### Service and Service Group Overview

---

You can use the Service Creation Wizard to create a service object based on the protocols the service uses. The protocols that are used to create an service object include:

- TCP
- UDP
- MS-RPC
- SUN-RPC
- ICMP
- ICMPv6

You can group service objects to form a service group using the Service Group Creation Wizard. Junos Space creates an object in the Junos Space database to represent an service or an service group.

There are Juniper Networks defined service objects for commonly used services.



NOTE: You cannot modify or delete Juniper Networks defined service objects.

#### Related Documentation

- [Creating Services on page 22](#)
- [Creating Service Groups on page 27](#)
- [Managing Services on page 25](#)
- [Managing Service Groups on page 28](#)

## Creating Services

To create a service:

1. From the **Security Design** task ribbon, select **Object Builder > Services**.

The **Manage Services** page appears, listing all available services.

2. From the taskbar, select the Create Service icon.

The **Create Service** page appears, as shown in [Figure 4 on page 22](#). Click on the plus sign (+).

Figure 4: Create Service: Basic View Page

The screenshot shows the 'Create Service' interface. The main window has a dark blue header with the title 'Create Service'. Below the header, there are two text input fields: 'Name' and 'Description'. Underneath these is a 'Protocols' section with a plus icon, a pencil icon, and a minus icon. Below this is a table with columns 'Name', 'Description', 'Type', and 'Detail'. At the bottom of the page are 'Create' and 'Cancel' buttons. A 'New Protocol' dialog box is open on the right side of the page. The dialog box has a title bar 'New Protocol' and a close button. It contains input fields for 'Name' and 'Description', a 'Type' dropdown menu set to 'TCP', and a 'Destination Port' input field. Below these is a checkbox labeled 'Advanced Settings'. At the bottom of the dialog box are 'Add' and 'Cancel' buttons.

3. Click on the **Advanced Settings** to configure more parameters for the selected Type. However, this is not a mandatory field.



Figure 5: Create Service: Advanced Settings Page

The screenshot shows a 'New Protocol' dialog box. It has a title bar with the text 'New Protocol' and a close button. The main area contains the following fields:

- Name:** A text input field.
- Description:** A text area input field.
- Type:** A dropdown menu currently showing 'TCP'.
- Destination Port:** A text input field.
- Advanced Settings:** A section with a collapse icon, containing:
  - Disable Inactivity Timeout:** An unchecked checkbox.
  - Inactivity Timeout:** A text input field.
  - ALG:** A dropdown menu showing 'Please select'.
  - Source Port:** A text input field.

At the bottom of the dialog are two buttons: 'Add' (blue) and 'Cancel' (red).

4. Enter the name of the service in the **Name** field.
5. Enter a description for the service in the **Description** field.
6. In the **Protocols** pane, click Add icon to add a new protocol.

The **New Protocol** dialog box appears, populated with the default values.

7. Enter a name for the new protocol in the **Name** section.
8. Enter a description for the new protocol in the **Description** field.
9. Enter destination ports for the selected types in the **Destination Port** field.
10. Select a protocol type from the **Type** menu.

You can select the following protocol types from the **Type** menu:

- TCP
  - a. Select the appropriate option from the **ALG** menu.
  - b. Enter a range of TCP source ports in the **Source Port** field.
  - c. By default, **Disable Inactivity Timeout** check box is unchecked. Click the **Disable Inactivity Timeout** check box if you want to disable this option.
  - d. Enter a value, in seconds, in the **Inactivity Timeout** field.
- UDP

- a. Select the appropriate option from the **ALG** menu.
  - b. Enter a range of TCP source ports in the **Source Port** field.
  - c. By default, **Disable Inactivity Timeout** check box is unchecked. Click the **Disable Inactivity Timeout** check box if you want to disable this option.
  - d. Enter a value, in seconds, in the **Inactivity Timeout** field.
  - ICMP
    - a. Enter a value for the ICMP message you want to display in the **ICMP Type** field.
    - b. Enter a value for the ICMP type you have specified in the **ICMP Code** field.
  - SUN - RPC
    - a. Enter a value for the RPC service you want to use in the **RPC Program Number** field.
    - b. Select the **TCP** or **UDP** option button to specify an appropriate protocol type in the **Protocol Type** field.
  - MS - RPC
    - a. Enter the universally unique ID corresponding to the RPC service you want to use in the **UUID** field.
    - b. Select the **TCP** or **UDP** option button to specify an appropriate protocol type in the **Protocol Type** field.
  - ICMPv6
    - a. Enter a value for the ICMPv6 message you want to display in the **ICMP Type** field.
    - b. Enter a value for the ICMPv6 type you have specified in the **ICMP Code** field.
  - Other
    - a. Select the appropriate option from the **ALG** menu.
    - b. Enter a range of TCP source ports in the **Source Port** field.
    - c. Enter the number of the protocol in the **Protocol Number** field.

This number is specified in the **Protocol** field for IPv4 packets and the **Next Header** field for IPv6 packets.
    - d. By default, **Disable Inactivity Timeout** check box is unchecked. Click the **Disable Inactivity Timeout** check box if you want to disable this option.
    - e. Enter a value, in seconds, in the **Inactivity Timeout** field.
11. Click **Add** in the **New Protocol** dialog box.
  12. Click **Create** to create the service.

- Related Documentation**
- [Service and Service Group Overview on page 21](#)
  - [Creating Service Groups on page 27](#)
  - [Managing Services on page 25](#)
  - [Managing Service Groups on page 28](#)

## Managing Services

---

You can modify, delete, or clone services listed in the **Manage Service** page.

To open the **Manage Service** page:

- From the **Security Design** task ribbon, select **Object Builder > Services**.

The **Manage Services** page appears.

You can either right-click or use the Actions drawer to manage a service.

You can perform the following tasks on the **Manage Services** page:

1. [Modifying a Service on page 25](#)
2. [Deleting a Service on page 26](#)
3. [Cloning a Service on page 26](#)
4. [Find Duplicate Service Objects on page 26](#)

## Modifying a Service

To modify a service:

1. From the **Security Design** task ribbon, select **Object Builder > Services**.

The **Manage Services** page appears.

2. Select the service you want to modify and click the **Modify Service** link from the Actions drawer.

This action redirects you to the window that you used to create a new service. You can modify all the fields on this window, except the **Name** field.

3. In the **Category** field, enter a new category.
4. In the **Description** field, enter a new description.
5. Make necessary changes in the **Protocols** pane.
  - To edit a protocol, select the protocol you want to edit and click the **Edit** icon. Make the necessary changes and click **OK**.
  - To delete a protocol, select the protocol you want to delete and click the **Delete** icon.
6. Click **Modify** to save the changes made to this service.

## Deleting a Service

To delete a service:

1. From the **Security Design** task ribbon, select **Object Builder > Services**.  
The **Manage Services** page appears.
2. Select the service you want to delete and click the **Delete Services** link from the Actions drawer.  
The **Delete** dialog box appears
3. Select the service you want to delete and click **Delete**.

## Cloning a Service

To clone a service:

1. From the **Security Design** task ribbon, select **Object Builder > Services**.  
The **Manage Services** page appears.
2. Select the service you want to clone and click the **Clone Service** link from the Actions drawer.  
You are redirected to the **Clone Service** page.
3. Make necessary changes and click **Clone**.

## Find Duplicate Service Objects

To find duplicate service objects:

1. From the **Security Design** taskbar, select **Object Builder > Services**.  
The **Manage Services** page appears.
2. Select the service within which you want to find the duplicate objects. Right-click on the service, and then click **Show Duplicates**.  
A window appears, showing all the groups with that include duplicate objects.
3. If you want to merge duplicate objects in a group, select the objects in a group and click **Merge**.  
A merge window appears, as shown in the figure. In the **Name** field, provide a new object name or select existing object name from the list.



**NOTE:** You can merge all the objects in a group by clicking on **Merge** after selecting all the objects by clicking on the group name

---



**NOTE:** If the selected duplicate objects are referenced in any other services (firewall policy) and security objects (service groups), a warning message is provided before the objects are merged, as shown in the figure.

4. If you want to delete objects in a group, select an object or objects, right-click, and then select **Delete**. A confirmation window appears before the selected objects are deleted.

Click **Delete** to delete the selected objects or **Cancel** to cancel the deletion.

5. If you want to find the usage of the duplicate objects in other groups, select an object, right-click, and then select **Find Usage**.

The usage window appears, showing the usage of the selected object in any service (firewall policy), or security objects ( service groups) .

#### Related Documentation

- [Service and Service Group Overview on page 21](#)
- [Creating Services on page 22](#)
- [Creating Service Groups on page 27](#)
- [Managing Service Groups on page 28](#)

## Creating Service Groups

To create a service group:

1. From the **Security Design** task ribbon, select **Object Builder > Services**.

The **Manage Services** page appears with all the services and service groups.

2. From the task ribbon, select the **Create Service Group** icon.

The **Create Service Group** page appears, as shown in [Figure 6 on page 28](#).

Figure 6: Create Service Group Page

**Create Service Group**

Name:

Description:

Members:

Name	Description
apple-ichat	predefined service
biff	predefined service
bootpc	predefined service
cifs	predefined service

**Select Services**

Available:

Selected:

Available list: aol, apple-ichat-snatmap, bgp, bootps, chargen, cvspserver

Selected list: apple-ichat, biff, bootpc, cifs

3. In the **Name** field, enter a name for the new service group.
4. In the **Description** field, enter a description for the new service group.
5. In the **Members** pane, click the Add icon to add a new service to this service group.  
The **Select Services** dialog box appears.
6. From the **Available** pane in the dialog box, select the service you want to group, and click the Add icon.  
The service you have selected appears in the **Selected** section of the dialog box.  
Repeat Steps 5 and 6 to add more services to this service group.
7. Click **Create**.  
The service group appears in the **Manage Services** page.

#### Related Documentation

- [Service and Service Group Overview on page 21](#)
- [Managing Service Groups on page 28](#)
- [Creating Services on page 22](#)
- [Managing Services on page 25](#)

## Managing Service Groups

You can modify, delete, or clone service groups listed in the **Manage Services** page.

To open the **Manage Services** page:

- From the **Security Design** task ribbon, select **Object Builder > Services**.

The **Manage Services** page appears.

You can either right-click or use the Actions drawer to manage an service group.

You can perform the following tasks on the **Manage Services** page:

1. [Modifying a Service Group on page 29](#)
2. [Deleting a Service Group on page 29](#)
3. [Cloning a Service Group on page 29](#)

## Modifying a Service Group

To modify a service group:

1. From the **Security Design** task ribbon, select **Object Builder > Services**.  
The **Manage Services** page appears.
2. Select the service group you want to modify and click the **Modify Service** link from the Actions drawer.  
This action redirects you to the window that you used to create a new service group. You can modify all the fields on this window, except the **Name** field.
3. In the **Description** field, enter a new description.
4. In the **Category** field, enter a new category.
5. In the **Members** section, make appropriate changes to the services used in this group.
6. Click **Modify** to save the changes made to this service group.

## Deleting a Service Group

To delete a service group:

1. From the **Security Design** task ribbon, select **Object Builder > Services**.  
The **Manage Services** page appears.
2. Select the service group you want to delete and click the **Delete Services** link from the Actions drawer.  
The **Delete** dialog box appears.
3. Select the service group you want to delete and click **Delete**.

## Cloning a Service Group

To clone a service group:

1. From the **Security Design** task ribbon, select **Object Builder > Services**.  
The **Manage Services** page appears.

2. Select the service group you want to clone and click the **Clone Service** link from the Actions drawer.

You are redirected to the **Clone Service** page.

3. Make necessary modifications and click **Clone**.

**Related  
Documentation**

- [Service and Service Group Overview on page 21](#)
- [Creating Service Groups on page 27](#)
- [Creating Services on page 22](#)
- [Managing Services on page 25](#)



## CHAPTER 6

# Addresses and Address Groups

- [Address and Address Groups Overview on page 31](#)
- [Creating Addresses on page 31](#)
- [Managing Addresses on page 33](#)
- [Creating Address Groups on page 38](#)
- [Managing Address Groups on page 39](#)

## Address and Address Groups Overview

---

You can use the Address Creation Wizard to create an address object that specifies an IP address or a hostname. You can specify a hostname and use the address resolution option to resolve it to an IP address. You can also resolve an IP address to the corresponding hostname.

You can group address objects to form an address group using the Address Group Creation Wizard. Junos Space creates an object in the Junos Space database to represent an address or an address group.

### Related Documentation

- [Creating Addresses on page 31](#)
- [Managing Addresses on page 33](#)
- [Creating Address Groups on page 38](#)
- [Managing Address Groups on page 39](#)

## Creating Addresses

---

To create an address:

1. From the **Security Design** task ribbon, select **Object Builder > Addresses**.  
The **Manage Address** page appears.
2. From the task ribbon, select the **Create Address** icon.  
The **Create Address** page appears, as shown in [Figure 7 on page 32](#).

Figure 7: Create Address Page

3. In the **Name** field, enter a name for the new address.
4. In the **Description** field, enter a description for the new address.
5. Direct Security Design to resolve an IP address to a hostname or resolve a hostname to an IP address.
  - To specify an IP address as the address type, select **Host** from the drop-down menu and enter the IP address in the **IP** field.
  - To specify a hostname as the address type, select **Host** from the drop-down and enter the hostname in the **Host Name** field.
  - To specify an IP address range, select **Range** from the drop-down and enter the IP ranges in the **Start IP** and **End IP** fields.
  - To specify a network as an address type, select **Network** from the drop-down and enter the network address in the **IP** and **Netmask** fields.
  - To specify an IP address with a wildcard mask, select **Wildcard** from the drop-down and enter the IP address in the **IP** field and wildcard mask in the **Wildcard Mask** fields.
  - To specify a DNS name as an address type, select **DNS Host** from the drop-down menu and enter the DNS name in the **DNS Name** field.



**NOTE:** You can resolve an IP address to a hostname and a hostname to an IP address using the green arrows next to the IP and Host Name fields.



**NOTE:** The Host and Network address types support both IPv4 and IPv6 address types. It also supports multicast addresses. However the range address type supports only IPv4 addresses. NAT and IPsec VPNs do not support IPv6 addressing and wildcard addresses.



**NOTE:** Ensure that the first 8 bits of the address is not 0 and the highest bit of the mask is 1 when you are using wildcard address type.

6. Click **Create** to create an address.

The new address appears in the **Manage Address** page.



**NOTE:** You can also add addresses using the Address import functionality. To use this functionality, select the Actions drawer and click **Import Addresses from CSV**.



**NOTE:** You can export the addresses using the Address export functionality. To use this functionality, select the addresses you want to export and select **Export Addresses to CSV** from the Actions drawer.

#### Related Documentation

- [Address and Address Groups Overview on page 31](#)
- [Managing Addresses on page 33](#)
- [Creating Address Groups on page 38](#)
- [Managing Address Groups on page 39](#)

## Managing Addresses

You can modify, delete, clone, export, and import addresses listed in the **Manage Address** page.

To open the **Manage Address** page:

- From the **Security Design** task ribbon, select **Object Builder > Addresses**.

The **Manage Address** page appears.

You can either right-click or use the Actions drawer to manage an address.

You can perform the following tasks on the **Manage Address** page:

1. [Modifying an Address on page 34](#)
2. [Deleting an Address on page 34](#)
3. [Cloning an Address on page 34](#)
4. [Exporting Addresses on page 35](#)
5. [Importing Addresses on page 35](#)
6. [Find Duplicate Address Objects on page 35](#)

## Modifying an Address

To modify an address:

1. From the **Security Design** task ribbon, select **Object Builder > Addresses**.

The **Manage Address** page appears.

2. Select the address you want to modify and click the **Modify Address** link from the Actions drawer.

This action redirects you to the window that you used to create a new address. You can modify all the fields in this window, except the **Name** field.

3. In the **Description** field, enter a new description.
4. Enter a new value for the address type you specified earlier in the appropriate field (**IP Address** field if you choose IP Address as the address type or hostname if you have chosen **Hostname** ).
5. Click **Modify** to save the changes made to this address.

## Deleting an Address

To delete an address:

1. From the **Security Design** task ribbon, select **Object Builder > Addresses**.

The **Manage Address** page appears.

2. Select the address you want to delete and click the **Delete Addresses** link from the Actions drawer.

The **Delete** dialog box appears.

3. Select the address you want to delete and click **Delete**.

## Cloning an Address

To clone an address:

1. From the **Security Design** task ribbon, select **Object Builder > Addresses**.

The **Manage Address** page appears.

2. Select the address you want to clone and click the **Clone Address** link from the Actions drawer.

You are redirected to the **Clone Address** page.

3. Make necessary modifications and click **Clone**.

## Exporting Addresses

To export addresses:

1. From the **Security Design** task ribbon, select **Object Builder > Addresses**.  
The **Manage Address** page appears.
2. Select the addresses you want to export and click the **Export Addresses to CSV** link from the Actions drawer.  
The **Export Addresses** pop-up window appears.
3. Click **Export Selected** to export the addresses you have selected.
4. If you want to export all addresses to CSV, click the **Export Addresses to CSV** link from the Actions drawer and click **Export All** from the **Export Addresses** pop-up window.

## Importing Addresses

To import addresses:

1. From the **Security Design** task ribbon, select **Object Builder > Addresses**.  
The **Manage Address** page appears.
2. Click the **Import Addresses from CSV** link from the Actions drawer.  
The **Select CSV File** window appears.
3. Click the **View Sample CSV** link to view a sample CSV file.
4. Click **Browse** and navigate to the location where you saved the CSV file.
5. Click **OK** and then click **Import**.

## Find Duplicate Address Objects

To find duplicate address objects:

1. From the **Security Design** taskbar, select **Object Builder > Addresses**.  
The **Manage Address** page appears.
2. Select the address for which you want to find the duplicate objects. Right-click on the address, and then click **Show Duplicates**.

A window appears showing all the groups with duplicate objects, as shown in [Figure 8 on page 36](#).

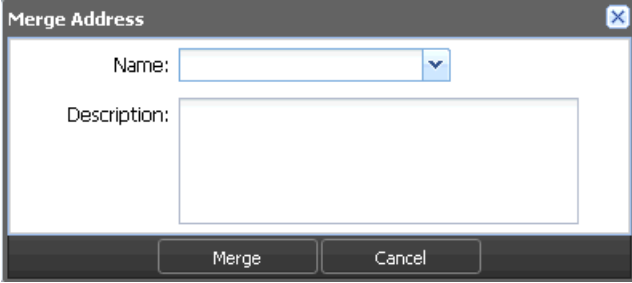
Figure 8: Page Showing Duplicate Address Objects

Name	Type	Host Name	IP Address	Description	
1.1.1.1 (2 members)					Merge
Copy_of_host	Host		1.1.1.1		
host	Host		1.1.1.1		
2.2.2.0-2.2.2.20 (2 members)					Merge
3.3.3.0/24 (2 members)					Merge
10.0.0.0/255.0.0.255 (2 members)					Merge
dns (2 members)					Merge
4.4.4.0-4.4.4.255 (2 members)					Merge
2::2 (2 members)					Merge
2::0/20 (2 members)					Merge
emptygrp1 (2 members)					Merge
group1 (2 members)					Merge

- If you want to merge duplicate objects in a group, select the objects in a group and click **Merge**.

A merge window appears as shown in [Figure 9 on page 36](#). In the **Name** field, provide a new object name or select existing object names from the list.

Figure 9: Merge Address Page



The dialog box titled "Merge Address" contains a "Name:" label with a text input field and a dropdown arrow. Below it is a "Description:" label with a larger text input area. At the bottom are "Merge" and "Cancel" buttons.

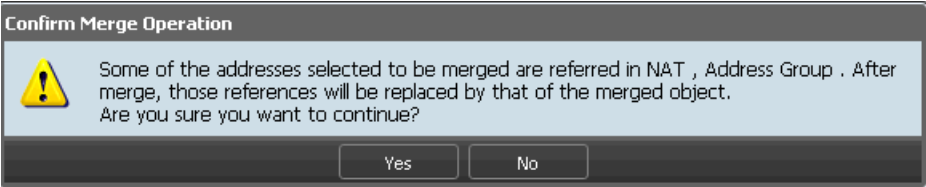


**NOTE:** You can merge all the objects in a group by clicking on the **Merge** button after selecting all the objects by clicking on the group name.



**NOTE:** If the selected duplicate objects are referenced in any other services (firewall policy, NAT policy, or VPN), and security objects (NAT pool, address groups), a warning message is provided before the objects are merged, as shown in [Figure 10 on page 36](#).

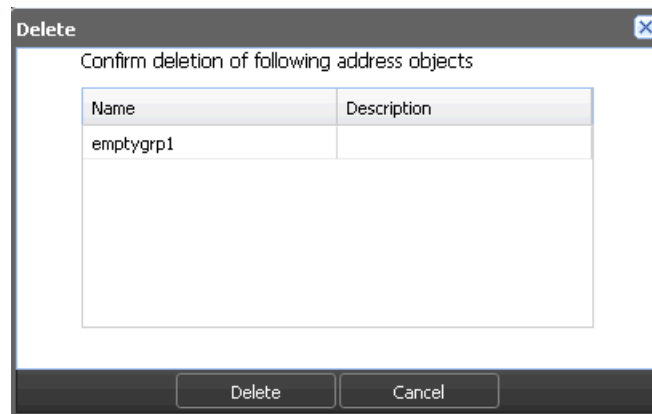
Figure 10: Merge Operation Confirmation Message



The dialog box titled "Confirm Merge Operation" features a yellow warning triangle icon. The text inside reads: "Some of the addresses selected to be merged are referred in NAT , Address Group . After merge, those references will be replaced by that of the merged object. Are you sure you want to continue?". At the bottom are "Yes" and "No" buttons.

- If you want to delete objects in a group, select an object or objects, right-click and then select **Delete**. A confirmation window appears before the selected objects are deleted, as shown in [Figure 11 on page 37](#).

Figure 11: Duplicate Objects Delete Confirmation Page



Click **Delete** to delete the selected objects or **Cancel** to cancel the deletion.

5. If you want to find the usage of the duplicate objects in other groups, select an object, right-click, and then select **Find Usage**.

The usage window appears showing the usage of the selected object in any service ( firewall policy, NAT policy, or VPN), or security objects (NAT pool, address groups), as shown in [Figure 12 on page 37](#).

Figure 12: Duplicate Objects Usage Window



#### Related Documentation

- [Address and Address Groups Overview on page 31](#)
- [Creating Addresses on page 31](#)
- [Creating Address Groups on page 38](#)
- [Managing Address Groups on page 39](#)

## Creating Address Groups

To create an address group:

1. From the **Security Design** task ribbon, select **Object Builder > Address**.

The **Manage Address** page appears with the icons for all the addresses and address groups.

2. From the task ribbon, select the **Create Address Group** icon.

The **Create Address Group** page appears, as shown in [Figure 13 on page 38](#).

**Figure 13: Create Address Group Page**

Name	IP Address	Host Name	Type
64.5.195.25	64.5.195.25		Host
64.5.145.253	64.5.145.253		Host
64.4.111.0_27	64.4.111.0/27		Netw
10.159.2.0/25	10.159.2.0/25		Netw
64.34.14.0/24	64.34.14.0/24		Netw
64.74.223.36/	64.74.223.36		Host
64.74.80.0/24	64.74.80.0/24		Netw

3. In the **Name** field, enter a name for the new address group.
4. In the **Description** field, enter a description for the new address group.
5. In the **Addresses** pane of the **Create Address Group** window, click the **Add** icon to add a new address to this address group.

The **Select Addresses** dialog box appears.

6. Select the addresses you want to add to the address group and click **Select**.
7. Click **Create**.

The address group appears in the **Manage Address** page.

### Related Documentation

- [Address and Address Groups Overview on page 31](#)
- [Managing Address Groups on page 39](#)
- [Creating Addresses on page 31](#)
- [Managing Addresses on page 33](#)



## Managing Address Groups

---

You can modify, delete, or clone address groups listed in the **Manage Address** page.

To open the **Manage Address** page:

- From the **Security Design** task ribbon, select **Object Builder > Address**.

The **Manage Address** page appears.

You can either right-click or use the Actions drawer to manage an address group.

You can perform the following tasks on the **Manage Address** page:

1. [Modifying an Address Group on page 39](#)
2. [Deleting an Address Group on page 39](#)
3. [Cloning an Address Group on page 40](#)

### Modifying an Address Group

To modify an address group:

1. From the **Security Design** task ribbon, select **Object Builder > Addresses**.

The **Manage Address** page appears.

2. Select the address group you want to modify and click the **Modify Address** link from the Actions drawer.

This action redirects you to the window that you used to create a new address group. You can modify all the fields in this window, except the **Name** field.

3. In the **Description** field, enter the new description.
4. In the **Members** pane, make appropriate changes to the addresses used in this group.
5. Click **Modify** to save the changes made to this address group.

### Deleting an Address Group

To delete an address group:

1. From the **Security Design** task ribbon, select **Object Builder > Addresses**.

The **Manage Address** page appears.

2. Select the address you want to delete and click the **Delete Addresses** link from the Actions drawer.

The **Delete** dialog box appears.

3. Select the address group you want to delete and click **Delete**.

## Cloning an Address Group

To clone an address group:

1. From the **Security Design** task ribbon, select **Object Builder > Addresses**.

The **Manage Address** page appears.

2. Select the address you want to clone and click the **Clone Addresses** link from the Actions drawer.

You are redirected to the **Clone Address** page.

3. Make necessary modifications and click **Clone**.

### Related Documentation

- [Address and Address Groups Overview on page 31](#)
- [Creating Address Groups on page 38](#)
- [Creating Addresses on page 31](#)
- [Managing Addresses on page 33](#)

## CHAPTER 7

# Extranet Devices

- [Creating Extranet Devices on page 41](#)
- [Managing Extranet Devices on page 42](#)

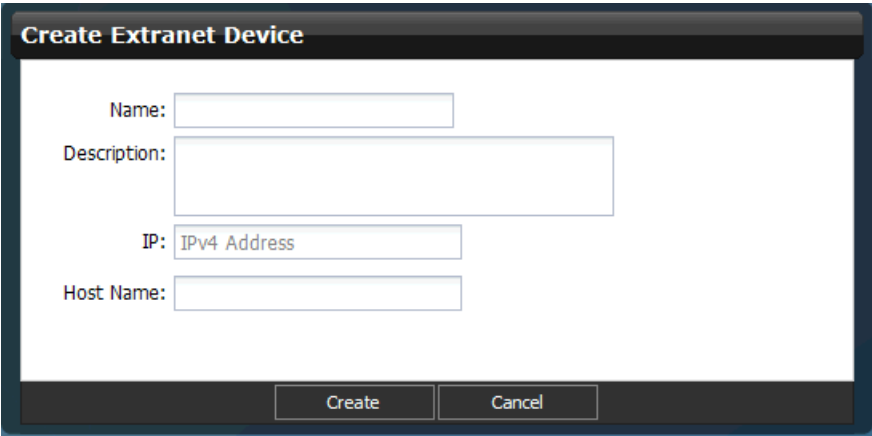
### Creating Extranet Devices

---

To create extranet devices:

1. From the **Security Design** taskbar, select **Object Builder > Extranet Devices**.  
The **Manage Address** page appears.
2. From the taskbar, select the **Create Extranet Device** icon.  
The **Create Extranet Device** page appears, as shown in [Figure 14 on page 41](#).

Figure 14: Create Extranet Device Page



3. In the **Name** field, enter a name for the new extranet device.
4. In the **Description** field, enter a description for the new extranet device.
5. In the **IP** field, enter the IP address.
6. In the **Host Name** field, enter the hostname.
7. Click **Create** to create the extranet device.

The new extranet device appears in the **Manage Address** page.

- Related Documentation**
- [Managing Extranet Devices on page 42](#)

---

## Managing Extranet Devices

You can modify, delete, and clone the extranet devices listed in the **Manage Extranet Devices** page.

To open the **Manage Extranet Devices** page:

- From the **Security Design** taskbar, select **Object Builder > Extranet Devices**.

The **Manage Extranet Devices** page appears.

You can either right-click or use the Actions drawer to manage an extranet device.

You can perform the following tasks on the **Manage Extranet Devices** page:

- [Modifying an Extranet Device on page 42](#)
- [Deleting an Extranet Device on page 42](#)
- [Cloning an Extranet Device on page 43](#)

### Modifying an Extranet Device

To modify an extranet device:

1. From the **Security Design** taskbar, select **Object Builder > Extranet Devices**.

The **Manage Extranet Devices** page appears.

2. Select the extranet device you want to modify, and click the **Modify Extranet Device** link from the Actions drawer.

This action redirects you to the Create Extranet Device page that you used to create a new extranet device. You can modify all the fields on this page.

3. Click **Modify** to save the changes made to this extranet device.

### Deleting an Extranet Device

To delete an extranet device:

1. From the **Security Design** taskbar, select **Object Builder > Extranet Devices**.

The **Manage Extranet Devices** page appears.

2. Select the extranet device you want to delete, and click the **Delete Extranet Devices** link from the Actions drawer.

The **Delete** dialog box appears.

3. Select the extranet devices you want to delete, and click **Delete**.

## Cloning an Extranet Device

1. From the **Security Design** taskbar, select **Object Builder > Extranet Devices**.

The **Manage Extranet Devices** page appears.

2. Select the extranet device you want to clone, and click the **Clone Extranet Device** link from the Actions drawer.

You are redirected to the **Clone Extranet Device** page.

3. Make the necessary modifications, and click **Clone**.

### Related Documentation

- [Creating Extranet Devices on page 41](#)



## CHAPTER 8

# Application Signatures

- Creating Application Signatures on page 45
- Managing Application Signatures on page 47

## Creating Application Signatures

To create an application signature:

1. From the **Security Design** task ribbon, select **Object Builder > Application Signatures**.

All application signatures that are downloaded appears on the **Application Signatures** page as shown in [Figure 15 on page 45](#). This page displays the version of the signature database. On the left side of the page are the different categories of signature and on the right side of the page are the signatures.

Figure 15: Application Signatures Page

Name	Category	Sub-Category	Risk	Pre-defined/Custom
163	Web	Portal	High	Pre-defined
2CH	Social-Networking		Low	Pre-defined
4CHAN	Social-Networking	Applications	Moderate	Pre-defined
4SHARED	Web	File-Sharing	Moderate	Pre-defined
4TUBE	Multimedia	Adult	Moderate	Pre-defined
9P	Infrastructure	Networking	Low	Pre-defined
AATK	Multimedia	Web-Based	Moderate	Pre-defined
ADDICTINGGAMES	Gaming	Web-Based	Low	Pre-defined
ADOBE-UPDATER	Infrastructure	Software-Update	Moderate	Pre-defined
ADRIIVE	Web	File-Sharing	Low	Pre-defined
ADULTFRIENDFINDER	Social-Networking	Applications	Low	Pre-defined
AFP	Infrastructure	File-Servers	Low	Pre-defined
AICOU-TIC	Infrastructure	Encryption	Low	Pre-defined
AIM	Messaging	Instant-Messaging	Critical	Pre-defined
AIMEXPRESS	Messaging	Instant-Messaging	Low	Pre-defined
ALLMUSIC-LOOKUP	Web	Search	High	Pre-defined
AMAZON	Web	Shopping	Critical	Pre-defined
AMEBA	Web	Blogging	Critical	Pre-defined

2. Click **Create Application Signature**.
- The **Create Application Signature** page appears.
3. Enter the name of the application signature in the **Name** field.
4. Enter the description for the application signature in the **Description** field.
5. Select the signature type.

6. If you select **Application** as the signature type, enter the following information:
  - a. Select the category of the application signature from the **Application Signature** drop-down menu.
  - b. Select the subcategory of the application signature from the **Sub-Category** drop-down menu.
  - c. Select the category of risk from the **Risk** drop-down menu, as shown in [Figure 16 on page 46](#).



Figure 16: Create Application Signature Page

**Create Application Signature**

Name:

Description:

Signature type:

 Application       Nested Application

Tags

Category:  Sub-Category:  Risk:

Pattern-0

Signature Details

Min Data:  Port Range:

CTS Pattern:

STC Pattern:

Create Cancel

- d. Enter appropriate information in the **Min Data** field.
  - e. Enter the range of ports in the **Port Range** field.
  - f. Enter appropriate information in the **CTS Pattern** field.
  - g. Enter appropriate information in the **STC Pattern** field.
  - h. Click **Create**.
7. If you select **Nested Application** as the signature type, enter the following information.



- a. Select the category of the application signature from the **Application Signature** drop-down menu.
- b. Select the subcategory of the application signature from the **Sub-Category** drop-down menu.
- c. Select the category of risk from the **Risk** drop-down menu.
- d. Click the check box next to the **Chain Order** field if you want to do so.
- e. Enter the range of ports in the **Max Transactions** field.
- f. Select the type of protocol from the **Protocol** drop-down menu.
- g. Select the context of the signature from the **Context** drop-down menu.
- h. Select the direction from the **Direction** drop-down menu.
- i. Enter appropriate information in the **Pattern** field.
- j. Click the **Add Signature** button to add more signature.
- k. Click **Create**.

**Related  
Documentation**

- [Managing Application Signatures on page 47](#)

---

## Managing Application Signatures

You can filter, modify, delete, or clone, application signatures listed in the **View All App Signatures** page. You can also create application signature groups in this page.

To open the **View All App Signatures** page:

- From the **Security Design** task ribbon, select **Object Builder > Application Signatures**.

The **View All App Signatures** page appears.

You can either right-click or use the Actions drawer to manage application signatures.

You can perform the following tasks in the **View All App Signatures** page:

- [Filtering Application Signatures on page 47](#)
- [Modifying Application Signatures on page 48](#)
- [Deleting Application Signatures on page 48](#)
- [Cloning Application Signatures on page 48](#)
- [Creating an Application Signature Group on page 49](#)

## Filtering Application Signatures

To filter application signatures:

1. From the **Security Design** task ribbon, select **Object Builder > Application Signatures**.

The **View All App Signatures** page displays all signatures that are downloaded. The right pane displays the signatures and the left pane displays the different filters that can be used to filter the signatures. The different parameters that can be used to filter the signatures include Category, Sub-Category, and Risk, Predefined/Custom, Object Type, Activation Date, and Modify Date. Every parameter has different subparameters.

2. Click the check box next to the subparameters within a parameter.

## Modifying Application Signatures

To modify application signatures:

1. From the **Security Design** task ribbon, select **Object Builder > Application Signatures**.

The **View All App Signatures** page displays all signatures that are downloaded.

2. Select the check box next to the application signature you want to modify.



**NOTE:** You cannot modify the predefined application signatures. You can only modify the custom application signatures you have added.

3. Click **Modify Application Signature** in the Actions drawer.

You will be redirected to the **Modify Application Signature** page. You can make necessary changes to the application signature here.

4. Click **Modify**.

## Deleting Application Signatures

To delete application signatures:

1. From the **Security Design** task ribbon, select **Object Builder > Application Signatures**.

The **View All App Signatures** page displays all signatures that are downloaded.

2. Select the check box next to the application signatures you want to delete.



**NOTE:** You cannot delete the predefined application signatures. You can only delete the custom application signatures you have added.

3. Click **Delete Selected** in the Actions drawer.

A confirmation window appears.

4. Click **Yes**.

## Cloning Application Signatures

To clone application signatures:

1. From the **Security Design** task ribbon, select **Object Builder > Application Signatures**.

The **View All App Signatures** page displays all signatures that are downloaded.

2. Select the check box next to the application signature you want to clone.
3. Click **Clone Application Signature** in the Actions drawer.

You are redirected to the **Create Application Signature** page. You can create the application signature here.

## Creating an Application Signature Group

To create an application signature group:

1. From the **Security Design** task ribbon, select **Object Builder > Application Signatures**.

The **View All App Signatures** page displays all signatures that are downloaded.

2. Select the check box next to the application signatures you want to include in the application signature group.
3. Click **Create Application Group** from the Actions drawer.

The **Create Application Signature Group** page appears.

4. Enter a name for the application signature group in the **Name** field.
5. Click the check box next to the **Disable** option if you want to disable this application signature group.
6. Click the Add icon to add more application signatures to this group.

The **Application Signature Selector** window appears. You can add more application signatures from this window.

7. Click **Update**.
8. Click **Create**.



## CHAPTER 9

# NAT Pools

- [Creating NAT Pools on page 52](#)
- [Managing NAT Pools on page 53](#)

## Creating NAT Pools

A Network Address Translation (NAT) pool is a continuous range of IP addresses that you can use to create a NAT policy. NAT policies perform address translation by translating internal IP addresses to the addresses in these pools.

To create a NAT pool:

1. From the **Security Design** task ribbon, select **Object Builder > NAT Pools > Create NAT Pool**.

The **Create NAT Pool** page appears, as shown in [Figure 17 on page 52](#).

Figure 17: Create NAT Pool Page

2. Enter the name of the NAT pool in the **Name** field.
3. Enter a description for the NAT pool in the **Description** field.
4. Select the type of NAT pool from the **Pool Type** menu.
5. Select the appropriate address from the **Pool Address** menu.
6. Expand the **Routing Instance** pane by clicking on the down arrow.
7. Select the device from the **Device** list. **Routing Instance** field lists the available routing instances for the selected devices.
8. Select the desired routing instance for the selected device from the routing instances listed.

9. Expand the **Advanced** pane by clicking the down arrow.
10. Enter an appropriate value in the **Host Address Base** field.
11. Select the appropriate option from the **Translation** menu.
  - If you select **Port/Range** in the **Translation** menu, a new menu, **Port**, appears.
  - Select an appropriate option from the **Port** menu.
  - If you select **Overload** in the **Translation** menu, a new option, **Port Overloading Factor**, appears.
  - Select an appropriate value from the **Port Overloading Factor** selector.
12. Select the appropriate option from the **Overflow Pool Type** menu.
  - If you select **Pool** in the **Overflow Pool Type** menu, a new field, **Overflow Pool**, appears.
  - Select the appropriate NAT pool from the **Overflow Pool** selector.
13. Click **Create**.

**Related  
Documentation**

- [NAT Overview on page 149](#)
- [Managing NAT Pools on page 53](#)
- [Creating NAT Policies on page 151](#)
- [Managing NAT Policies on page 163](#)

---

## Managing NAT Pools

You can delete, modify, and clone NAT pools listed in the **Manage NAT Pool** page.

To open the **Manage NAT Pool** page:

- From the **Security Design** task ribbon, select **Object Builder > NAT Pool**.

The **Manage NAT Pool** page appears.

You can either right-click or use the Actions drawer to manage a NAT pool.

You can perform the following tasks on the **Manage NAT Pool** page:

- [Deleting NAT Pools on page 53](#)
- [Modifying NAT Pools on page 54](#)
- [Cloning NAT Pools on page 54](#)

## Deleting NAT Pools

To delete a NAT pool:

1. From the **Security Design** task ribbon, select **Object Builder > NAT Pools**.  
The **Manage NAT Pool** page appears.

2. Select the NAT pool that you want to delete and click **Delete NAT Pools** from the Actions drawer.

The **Delete** pop-up window appears displaying all the NAT pools that you want to delete.

3. Click **Delete**.



**NOTE:** You cannot delete a NAT pool that is associated with a NAT policy.

## Modifying NAT Pools

To modify a NAT pool:

1. From the Security Design task ribbon, select **Object Builder > NAT Pools**. The **Manage NAT Pool** page appears.
2. Select the NAT pool that you want to modify and click **Modify NAT Pool** from the Actions drawer.

The **Modify NAT Pool** page appears.

3. On the **Modify NAT Pool** page, you can edit the description and IP range of the NAT pool. You cannot modify the NAT pool name.
4. Click **Modify**.

You will receive a warning message when you try to modify a NAT pool used in a NAT policy. When you modify a pool associated with a published policy, you must republish the policy so that the changes are reflected in the policy.

## Cloning NAT Pools

To clone a NAT pool:

1. From the Security Design task ribbon, select **Object Builder > NAT Pools**. The **Manage NAT Pools** page appears.
2. Select the NAT pool you want to clone and click **Clone NAT Pool** from the Actions drawer.

The **Clone NAT Pool** window appears.

3. Make appropriate changes and save the NAT pool.



**NOTE:** You can also clone the NAT pool by right-clicking the NAT pool and selecting the **Clone NAT Pool** option.

- Related Documentation**
- [NAT Overview on page 149](#)
  - [Creating NAT Pools on page 52](#)



- [Creating NAT Policies on page 151](#)
- [Managing NAT Policies on page 163](#)



## CHAPTER 10

# Policy Profiles

- [Security Policy Profiles Overview on page 57](#)
- [Creating Policy Profiles on page 58](#)
- [Managing Policy Profiles on page 60](#)

### Security Policy Profiles Overview

---

You can use the Policy Profile Wizard to create an object that specifies the basic settings of a security policy. You can configure these basic settings using the Policy Profile Wizard:

- Log options
  - Log at session initiation
  - Log at the close of a session
  - Enable counting for the number of packets, bytes, and sessions that enter the firewall for a given policy
- Firewall authentication schemes
  - Pass through authentication
  - Web authentication
  - Infranet authentication
- Traffic redirection options
  - No traffic redirection
  - Redirect Wx — Wx redirection for packets that arrive from the LAN
  - Reverse Redirect Wx — Wx redirection for the reverse flow of packets that arrive from the WAN

When a policy profile is created, Junos Space creates an object in the Junos Space database to represent the policy profile. You can use this object to create security policies.

There are two Juniper Networks defined policy profiles:

- All logging enabled — All logging options are enabled. Logging is enabled at session initiation and the close of the session. Counters are also enabled to collect the number of packets, bytes, and sessions that enter the firewall for a given policy. The alarm thresholds are set to 100 bytes/second and 100 kilobytes/minute.
- All logging disabled — All logging options are disabled.



**NOTE:** You cannot modify or delete Juniper Networks defined policy profiles. You can only copy them and create new policy profiles.

**Related  
Documentation**

- [Creating Policy Profiles on page 58](#)
- [Managing Policy Profiles on page 60](#)

---

## Creating Policy Profiles

To create a security policy profile:

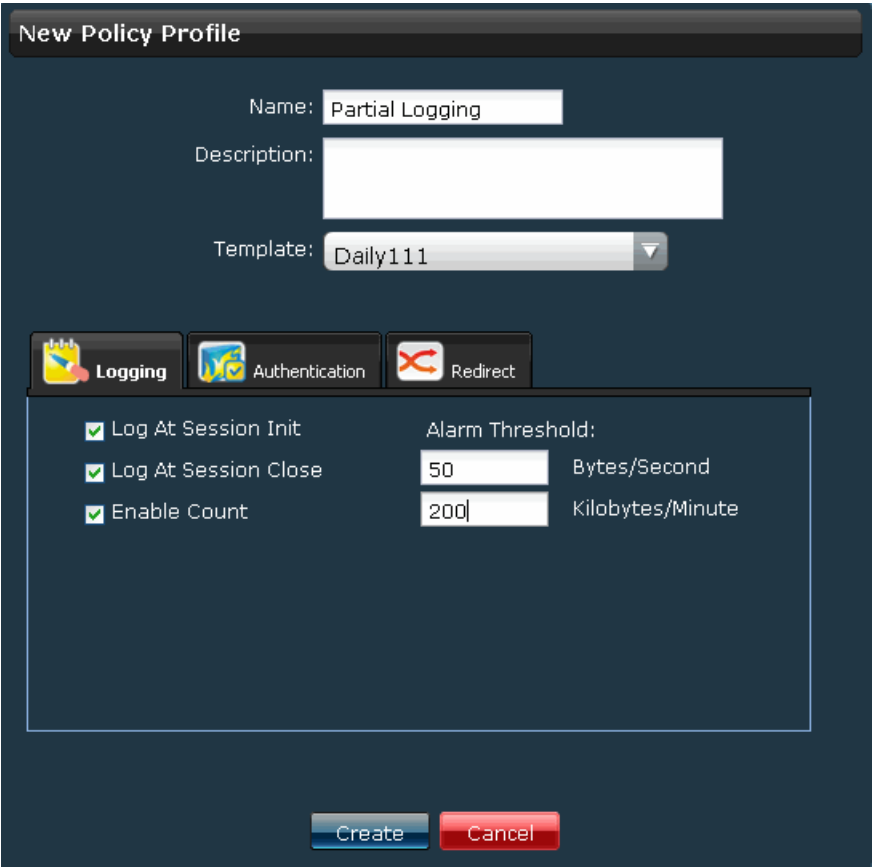
1. From the **Security Design** task ribbon, select **Object Builder > Policy Profiles**.

The **Manage Policy Profiles** page appears with all the policy profiles. The first two policy profiles listed here are Juniper Networks defined policy profiles.

2. From the task ribbon, select the **Create Policy Profile** icon.

The **New Policy Profile** page appears, as shown in [Figure 18 on page 59](#).

Figure 18: New Policy Profile Page



**New Policy Profile**

Name:

Description:

Template:

**Logging** **Authentication** **Redirect**

☒ Log At Session Init

☒ Log At Session Close

☒ Enable Count

Alarm Threshold:

Bytes/Second

Kilobytes/Minute

3. Enter the name of the policy profile in the **Name** field.
4. Enter the description of the policy profile in the **Description** field.
5. In the **Logging** pane of the **New Policy Profile** page, configure the log options for this policy profile. You can configure the following log options:
  - a. Select the **Log at Session Init** check box if you want to log the events when the session is created.
  - b. Select the **Log at Session Close** check box if you want to log the events when the session is closed.
  - c. Enter the number of bytes to be logged per second in the **Bytes/Second** field.
  - d. Select the **Enable Count** check box if you want to enable counting.  
If counting is enabled, counters are collected for the number of packets, bytes, and sessions that enter the firewall for a given policy
  - e. Enter the value of the count in the **Kilobytes/Minute** field.
6. Use the **Authentication** pane of the **New Policy Profile** page to provide authentication to clients. You can configure the following authentication options:

- a. If you want to use Web Authentication, select **Web** in the **Authentication Type** drop-down menu and enter the hostname or IP address of the client used to perform Web authentication in the **Client Name** field.
  - b. If you want to use Pass Through Authentication, select **Pass Through** in the **Authentication Type** drop-down menu and enter the hostname or IP address of the client used to perform Pass Through authentication in the **Client Name** field.
  - c. If you do not want to use any authentication, select **None** in the **Authentication Type** drop-down menu.
  - d. If you want to use Infranet Authentication, select **Infranet** in the **Authentication Type** drop-down menu and enter the Redirect URL in the **Redirect URL** field. You can also select the appropriate redirect options from the respective check boxes.
7. Use the **Redirect** section of the **New Policy Profile** page to configure the traffic redirection options for this policy profile.
    - a. If you want traffic to be redirected, select the **None** check box.
    - b. If you want to enable Wx redirection for packets that arrive from the LAN, select the **Redirect Wx** check box.
    - c. If you want to enable Wx redirection for the reverse flow of packets that arrive from the WAN, select the **Reverse Redirect Wx** check box.
  8. Click **Create**.

The new security policy profile appears in the **Manage Policy Profiles** page.

- Related Documentation**
- [Security Policy Profiles Overview on page 57](#)
  - [Managing Policy Profiles on page 60](#)

---

## Managing Policy Profiles

You can delete, modify, or clone policy profile listed in the **Policy Profiles** page.

To open the **Policy Profiles** page:

- From the **Security Design** task ribbon, select **Object Builder > Policy Profiles**.

The **Policy Profiles** page appears.

You can either right-click or use the Actions drawer to manage a policy profile.

You can perform the following tasks on the **Policy Profiles** page:

- [Deleting Policy Profiles on page 61](#)
- [Modifying Policy Profiles on page 61](#)
- [Cloning Policy Profiles on page 61](#)

## Deleting Policy Profiles

To delete a policy profile:

1. From the **Security Design** task ribbon, select **Object Builder > Policy Profiles**.

The **Manage Policy Profiles** page appears.

2. Select the policy profile that you want to delete and select **Delete Policy Profiles** from the Actions drawer.

The **Delete** pop-up window appears.

3. Select the security policy profiles you want to delete and click **Delete**.



**NOTE:** You can also delete the policy profile by right-clicking the policy profile and selecting **Delete Policy Profiles**.

## Modifying Policy Profiles

To modify a policy profile:

1. From the **Security Design** task ribbon, select **Object Builder > Policy Profiles**.

The **Manage Policy Profiles** page appears.

2. Select the policy profile that you want to modify and select **Modify Policy Profile** from the Actions drawer.

The **Modify Policy Profile** page appears. You can modify all the fields on this window, except the **Name** field.

3. Make appropriate changes to security policy and click **Modify**.



**NOTE:** You can also modify the policy profile by right-clicking the policy profile and selecting **Modify Policy Profile**.

## Cloning Policy Profiles

To clone a policy profile:

1. From the **Security Design** task ribbon, select **Object Builder > Policy Profiles**.

The **Manage Policy Profiles** page appears.

2. Select the policy profile that you want to clone and select **Clone Policy Profile** from the Actions drawer.

The **Clone Policy Profile** page appears.

3. Make appropriate changes to security policy and click **Clone**.



.....

**NOTE:** You can also clone the policy profile by right-clicking the policy profile and selecting **Clone Policy Profile**.

.....



## CHAPTER 11

# VPN Profiles

- [VPN Profiles Overview on page 63](#)
- [Creating VPN Profiles on page 63](#)
- [Managing VPN Profiles on page 66](#)

## VPN Profiles Overview

---

You can use a VPN Profile Wizard to create an object that specifies the VPN proposals, mode of the VPN, and other parameters used in a route-based IPsec VPN. You can also configure the Phase 1 and Phase 2 settings in a VPN profile.

When a VPN profile is created, Junos Space creates an object in the Junos Space database to represent the VPN profile. You can use this object to create route-based IPsec VPNs.



**NOTE:** You cannot modify or delete Juniper Networks defined VPN profiles. You can only clone them and create new profiles.

### Related Documentation

- [Creating VPN Profiles on page 63](#)
- [Managing VPN Profiles on page 66](#)

## Creating VPN Profiles

---

To create a VPN profile:

1. From the **Security Design** task ribbon, select **Object Builder > VPN Profiles > Create VPN Profile**.

The **Manage VPN Profiles** page appears with all the VPN profiles. The first two profiles listed here are Juniper Networks defined VPN profiles.

2. Enter the name of the VPN profile in the **Name** field.
3. Enter the description of the VPN profile in the **Description** field.
4. Click the **Phase 1** tab.

The [Figure 19 on page 64](#) shows the Phase 1 tab.

Figure 19: VPN Profile: Phase 1

The screenshot shows the 'VPN Profile' configuration window with the 'Phase 1' tab selected. The 'Name' field is set to 'Bng\_IT' and the 'Description' field is empty. Under the 'Phase 1' tab, the 'Mode' is set to 'Aggressive' (radio button selected). The 'IKE Id' is set to 'Hostname' (dropdown menu). The 'Authentication Type' is 'Preshared Key'. The 'Proposals' are set to 'Predefined' (radio button selected). Below this, there are three radio buttons for 'Basic', 'Standard', and 'Compatible', with 'Basic' selected. An 'Advanced Settings' section is expanded, showing 'Enable NAT Traversal' checked, 'Keep Alive Interval(secs)' set to 5, 'Enable DPD' checked, 'Always Send DPD' unchecked, and 'DPD Interval(secs)' set to 10. At the bottom are 'Create' and 'Cancel' buttons.

5. Select the option button next to the VPN mode you want to use.
  - If you select **Aggressive** as the VPN mode, an **IKE ID** drop-down menu appears.
  - If you select the **User@hostname** option from the drop-down menu, a **User** field appears.
  - Enter the appropriate value in the **User@hostname** field.
6. Select the option button next to the VPN proposal you want to use.
 

If you select the **Custom** option button and want to create a custom proposal:

  - a. Click **Add** to add a new VPN proposal.
 

The **Create Phase 1 Proposal** pop-up window appears.
  - b. Enter the name for the proposal in **Name** field.
  - c. Select the appropriate DH group from the **DH Group** drop-down menu.
  - d. Select the appropriate authentication mechanism from the **Authentication** drop-down menu.
  - e. Select the appropriate encryption mechanism from the **Encryption** drop-down menu.
  - f. Select the life time interval from the **Life Time (in seconds)** selector.
  - g. Click **Create**.

7. Expand the **Advanced Settings** pane by clicking the down arrow.  
You can configure the advanced settings for Phase 1 here.
8. Select the **Enable NAT Traversal** check box to enable this option.
9. Select the appropriate keepalive interval from the **Keep Alive Interval (secs)** selector.
10. Select the **Enable DPD** check box if you want to use this option.
11. Select the **Always Send DPD** check box if you want to use this option.
12. Select the appropriate dead peer detection interval from the **DPD Interval (secs)** selector.
13. Select the appropriate dead peer detection threshold from the **DPD Threshold** selector.
14. Click the **Phase 2** tab.

Figure 20 on page 65 shows the Phase 2 tab.

**Figure 20: VPN Profile: Phase 2**

The screenshot shows the 'VPN Profile' configuration window with the 'Phase 2' tab selected. The 'Name' field is 'Bng\_IT' and the 'Description' field is empty. Under 'Proposals', 'Predefined' is selected, and 'Basic' is chosen from the sub-options. 'Perfect Forward Privacy' is set to 'None'. The 'Advanced Settings' pane is expanded, showing options: 'Establish tunnel immediately' (unchecked), 'Enable VPN Monitor' (unchecked), 'DF bit' set to 'None', 'Idle time(secs)' set to '60', 'Install time' set to '1', and 'Enable Anti Replay' (unchecked). 'Create' and 'Cancel' buttons are at the bottom.

15. Select the option button next to the VPN proposal you want to use.
16. Select an appropriate option from **Perfect Forward Privacy** drop-down menu.
17. Expand the **Advanced Settings** pane by clicking the down arrow.
18. Select the **Establish tunnel immediately** check box if you want to enable this option.
19. Select the **Enable VPN Monitor** check box if you want to enable this option.

This is a per-VPN option.

20. Select the appropriate option from the **DF Bit** drop-down menu.
21. Select the appropriate idle time interval from the **Idle time (secs)** selector.
22. Select the appropriate value from the **Install Time** selector.
23. Select the **Enable Anti Replay** check box if you to enable this option.
24. Click **Create**.

- Related Documentation**
- [VPN Profiles Overview on page 63](#)
  - [Managing VPN Profiles on page 66](#)

---

## Managing VPN Profiles

You can delete, modify, or clone VPN profiles listed in the **Manage VPN Profiles** page.

To open the **Manage VPN Profiles** page:

- From the **Security Design** task ribbon, select **Object Builder > VPN Profiles**.

The **Manage VPN Profiles** page appears.

You can either right-click or use the Actions drawer to manage a VPN profile.

You can perform the following tasks on the **Manage VPN Profiles** page:

- [Deleting VPN Profiles on page 66](#)
- [Modifying VPN Profiles on page 67](#)
- [Cloning VPN Profiles on page 67](#)

## Deleting VPN Profiles

To delete a VPN profile:

1. From the **Security Design** task ribbon, select **Object Builder > VPN Profiles**.  
The **Manage VPN Profiles** page appears.
2. Select the VPN profile you want to delete and click the **Delete VPN Profiles** link from the Actions drawer.  
The **Delete Profile** confirmation window appears.
3. Click **Delete**.



**NOTE:** You can also delete the VPN profile by right-clicking the VPN profile and selecting **Delete VPN Profiles**.

---

## Modifying VPN Profiles

To modify a VPN profile:

1. From the **Security Design** task ribbon, select **Object Builder > VPN Profiles**.  
The **Manage VPN Profiles** page appears.
2. Select the VPN profile you want to modify and click the **Modify VPN Profile** option from the Actions drawer.

You are redirected to the **Modify VPN Profile** page.

3. Click **Modify**.



**NOTE:** You can also modify the VPN profile by right-clicking the VPN profile and selecting **Modify VPN Profile**.



**NOTE:** If the VPN profile you have created is used as part of a VPN, you can modify all fields of the VPN profile except the Phase 1 IKE mode.

## Cloning VPN Profiles

To clone a VPN profile:

1. From the **Security Design** task ribbon, select **Object Builder > VPN Profiles**.  
The **Manage VPN Profiles** page appears.
2. Select the VPN profile you want to clone and click the **Clone VPN Profile** option from the Actions drawer.

You are redirected to the **Clone VPN Profile** page. By default, a generic name is given to the cloned VPN profile.



**NOTE:** You can also modify the VPN profile by right-clicking the VPN profile and selecting **Modify VPN Profile**.

3. Click **Clone**.



## CHAPTER 12

# Variables

- [Creating Variable Definitions on page 69](#)
- [Managing Variable Definitions on page 71](#)

### Creating Variable Definitions

---

To create variable definitions:

1. From the **Security Design** task ribbon, select **Object Builder > Variables**.

The **Manage Variables** page appears. This page displays all the variables you have created.

2. Click **Create Variable Definition**.

The **Create Polymorphic Object** page appears, as shown in [Figure 21 on page 70](#). You can create a variable definition on this page.

Figure 21: Create Polymorphic Object Page

**Create Polymorphic Object**

Name:

Description:

Type: ☒ Address ☐ Zone

Default Address:

Context Value	Address
---------------	---------

3. Enter the name of the variable definition in the **Name** field.
4. Enter a description for the variable definition in the **Description** field.
5. Select the type of variable definition, either Address or Zone, from the **Type** field.
6. Select the default address value from the **Default Address** menu.
7. To add variable values:
  - If the **Type** is Address:
    - a. Click the Add icon.  
A new row appears.
    - b. Double-click the **Context Value** field, and select the device.
    - c. Double-click the **Address** field, and select the address for the device from the menu.
  - If the **Type** is Zone:
    - a. Click the Add icon.  
A new row appears.



- b. Double-click the **Context Value** field, and select the device.
  - c. Double-click the **Zone** field, and select the zone, either trust or untrust, from the menu.
8. Click **Create**.



**NOTE:** You can search variables by name, description, or default value in the search box available at the top right corner of the **Manage Variables** page. If you want to tag the variables, right-click on the variable and select tag option. After tagging, you can search for variables by the respective tag names.

**Related Documentation**

- [Managing Variable Definitions on page 71](#)

## Managing Variable Definitions

You can delete, modify, or clone the variable definitions listed on the **Manage Variable Definitions** page.

To open the **Manage Variable Definitions** page:

- From the **Security Design** task ribbon, select **Object Builder > Manage Variable Definition**.

The **Manage Variable Definitions** page appears.

You can either right-click or use the Actions drawer to manage a variable definition.

You can perform the following tasks on the **Manage Variable Definitions** page:

- [Deleting Variable Definitions on page 71](#)
- [Modifying Variable Definitions on page 72](#)
- [Cloning Variable Definitions on page 72](#)

## Deleting Variable Definitions

To delete a variable definition:

1. From the **Security Design** task ribbon, select **Object Builder > Manage Variable Definition**.

The **Manage Variable Definitions** page appears. This page displays all the variable definitions you have created.

2. Select the variable definition you want to delete, and click **Delete Variable Definitions** from the Actions drawer.



**NOTE:** You can also delete the variable definition by right-clicking the variable definition and selecting **Delete Variable Definitions**. You can select more than one variable to delete.

## Modifying Variable Definitions

To modify a variable definition:

1. From the **Security Design** task ribbon, select **Object Builder > Manage Variable Definitions**.

The **Manage Variable Definitions** page appears. This page displays all the variable definitions you have created.

2. Select the variable definition you want to modify and click **Modify Variable Definition** from the Actions drawer.

The **Modify Variable Definitions** page appears. You can make the modifications on this page.



**NOTE:** You can also modify the variable definition by right-clicking the variable definition and selecting **Modify Variable Definition**.

3. Click **Modify**.

## Cloning Variable Definitions

To clone a variable definition:

1. From the **Security Design** task ribbon, select **Object Builder > Manage Variable Definitions**.

The **Manage Variable Definitions** page appears. This page displays all the variable definitions you have created.

2. Select the variable definition you want to clone and click **Clone Variable Definition** from the Actions drawer.

The **Clone Variable Definitions** page appears. You can make the modifications on this page.



**NOTE:** You can also clone the variable definition by right-clicking the variable definition and selecting **Clone Variable Definition**.

3. Click **Clone**.

# Template Definitions

- [Creating Template Definitions on page 73](#)
- [Managing Template Definitions on page 74](#)

## Creating Template Definitions

---

To create a Template Definition:

1. From the **Security Design** task ribbon, select **Object Builder > Manage Template Definitions**.

The **Manage Template Definitions** page appears. This page displays all the template definitions you have created.

2. Click **Create Template Definition**.

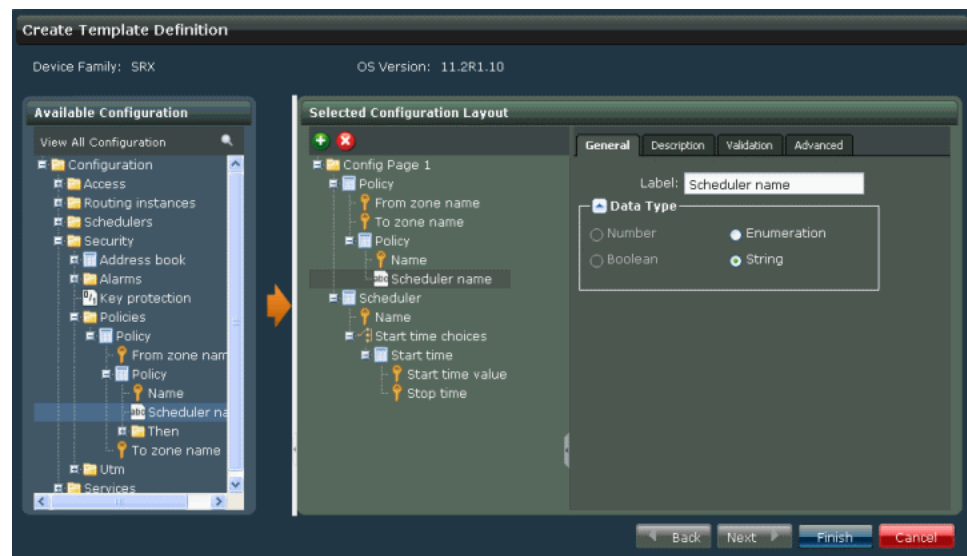
The **Create Template Definition** page appears.

3. Enter the name of the template definition in the **Name** field.
4. Enter a description for the template definition in the **Description** field.
5. Select the SRX schema version from the **SRX Schema Version** drop-down menu.
6. Click **Next**.

This page displays two sections: the **Available Configuration** pane on the left and the **Selected Configuration Layout** pane on the right. The **Available Configuration** pane displays the different configuration nodes. The **Select Configuration Layout** pane displays a default rule with “\$FromZone” for source zone and “\$ToZone” for destination zone.

7. Select the rule from the configuration node you want to add in the template definition and click the right arrow.
8. Modify the rule in the **Select Configuration Layout** pane, as shown in [Figure 22 on page 74](#).

Figure 22: Create Template Definition Page



9. Click **Finish**.

The new template definition is created.

**Related Documentation**

- [Managing Template Definitions on page 74](#)

## Managing Template Definitions

You can delete, or modify template definitions listed in the **Manage Variable Definitions** page.

To open the **Manage Template Definitions** page:

- From the **Security Design** task ribbon, select **Object Builder > Manage Template Definition**.

The **Manage Template Definitions** page appears.

You can either right-click or use the Actions drawer to manage a template definition.

You can perform the following tasks on the **Manage Template Definitions** page:

- [Deleting Template Definitions on page 74](#)
- [Modifying Template Definitions on page 75](#)

## Deleting Template Definitions

To delete a template definition:

1. From the **Security Design** task ribbon, select **Object Builder > Manage Template Definition**.

The **Manage Template Definitions** page appears. This page displays all the template definitions you have created.

2. Select the template definition you want to delete and click **Delete Template Definitions** from the Actions drawer.



**NOTE:** You can also delete the template definition by right-clicking the template definition and selecting **Delete Template Definitions**.

## Modifying Template Definitions

To modify a template definition:

1. From the **Security Design** task ribbon, select **Object Builder > Manage Template Definitions**.

The **Manage Template Definitions** page appears. This page displays all the template definitions you have created.

2. Select the template definition you want to modify and click **Modify Template Definition** from the Actions drawer.

The **Modify Template Definitions** page appears. You can make the modifications on this page.



**NOTE:** You can also modify the template definition by right-clicking the template definition and selecting **Modify Template Definition**.

3. Click **Modify**.



# Templates

- [Creating Templates on page 77](#)
- [Managing Templates on page 78](#)

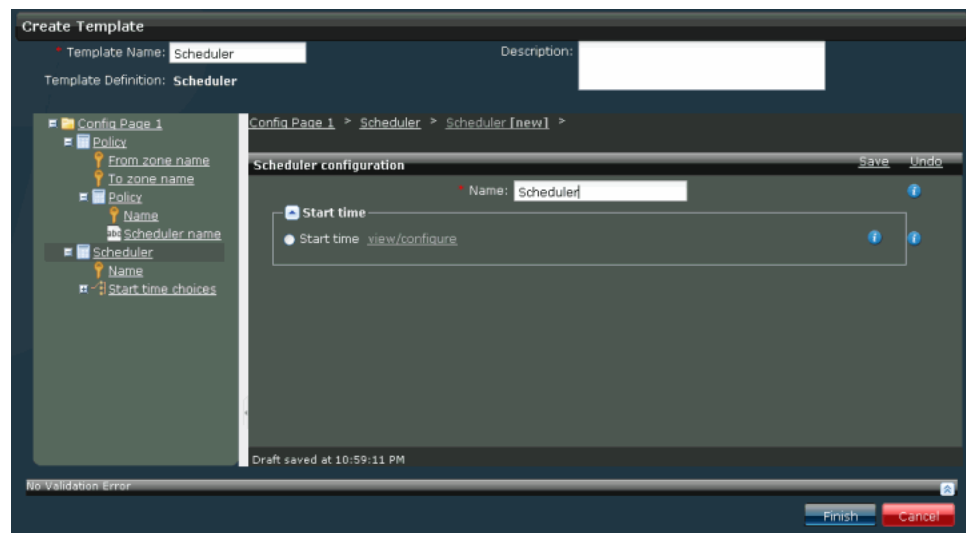
## Creating Templates

---

To create a template:

1. From the **Security Design** task ribbon, select **Object Builder > Manage Templates**.  
The **Manage Templates** page appears. This page displays all the templates you have created.
2. Click **Create Template**.  
The **Select Template Definition** page appears. You can create a template on this page.
3. Select an appropriate template definition and click **Next**.  
You can create a template on this page.
4. Enter the name of the template in the **Template Name** field.
5. Enter a description for the template in the **Description** field.
6. Select the configuration node from the left hand pane.
7. Select the appropriate value in the configuration node.
8. Modify the rule in the right pane, as shown in [Figure 23 on page 78](#).

Figure 23: Create Template Page



9. Click **Finish**.

**Related Documentation**

- [Managing Templates on page 78](#)

## Managing Templates

You can delete, or modify templates listed in the **Manage Templates** page.

To open the **Manage Templates** page:

- From the **Security Design** task ribbon, select **Object Builder > Manage Templates**.

The **Manage Template Definitions** page appears.

You can either right-click or use the Actions drawer to manage templates.

You can perform the following tasks on the **Manage Templates** page:

- [Deleting Templates on page 78](#)
- [Modifying Templates on page 79](#)

## Deleting Templates

To delete a template:

1. From the **Security Design** task ribbon, select **Object Builder > Manage Templates**.

The **Manage Templates** page appears. This page displays all the templates you have created.

2. Select the template you want to delete and click **Delete Templates** from the Actions drawer.





**NOTE:** You can also delete the template by right-clicking the template and selecting **Delete Templates**.

## Modifying Templates

To modify a template:

1. From the **Security Design** task ribbon, select **Object Builder > Manage Templates**.

The **Manage Templates** page appears. This page displays all the templates you have created.

2. Select the template you want to modify and click **Modify Template** from the Actions drawer.

The **Modify Templates** page appears. You can make the modifications on this page.



**NOTE:** You can also modify the template by right-clicking the template and selecting **Modify Template**.

3. Click **Modify**.



## PART 4

# Firewall Policy

- [Firewall Policy on page 83](#)



## CHAPTER 15

# Firewall Policy

- [Firewall Policies Overview on page 83](#)
- [Multiple Group Policy Membership Overview on page 85](#)
- [Global Address Book Overview on page 87](#)
- [Creating Firewall Policies on page 90](#)
- [Inline Creation of Objects in Policy on page 98](#)
- [Policy Priority Precedence Setting on page 103](#)
- [Adding Rules to a Firewall Policy on page 107](#)
- [Ordering the Rules in a Firewall Policy on page 110](#)
- [Publishing Firewall Policies on page 111](#)
- [Custom Columns in Firewall Policy on page 117](#)
- [Managing Firewall Policies on page 121](#)

## Firewall Policies Overview

---

Security Design provides you with four types of firewall policies:

- **All Devices**—Predefined firewall policy that is available with Security Design. You can add prerules, and postrules. When the all devices policy configuration is updated on the devices, the rules are updated in the following order:
  - All devices prerules
  - Group prerules
  - Device-specific rules
  - Group postrules
  - All devices postrules

All devices policy enables rules to be enforced globally to all the devices managed by Security Design.

- **Group**—Type of firewall policy that is shared with multiple devices. This type of policy is used when you want to update a specific firewall policy configuration to a large set of devices. You can create group prerules, group postrules, and device rules for a group

policy. When a group firewall policy is updated on the devices, the rules are updated in the following order:

- Group prerules
  - Device-specific rules
  - Group postrules
- Device Policy—Type of firewall policy that is created per device. This type of policy is used when you want to push a unique firewall policy configuration per device. You can create device rules for a device firewall policy.

Security Design views a logical system like it does any other security device, and it takes ownership of the security configuration of the logical system. In Security Design, each logical system is managed as a unique security device.



**NOTE:** If Security Design discovers the root logical system, the root lsys discovers all other user lsys inside the device.

---

- Device-exception Policy—Type of firewall policy that is created when a device is removed from a group policy.
- Global Policy—Global Policy Rules are enforced regardless of ingress or egress zones, they are enforced on any device transit. Any objects defined in the Global Policy Rules must be defined in the global address book.

Security Design permits users to manage the current zone-based firewall policies and the new Global policy rules supported in SRX Series devices. To achieve this the current policy model categorizes the rule bases into zone and global policies. Also, all the existing and new firewall policy features extends to global rule base. This includes the prerule or postrule predefined groups and the inheritance concept of current firewall policies. Because both the rule bases are managed within a single firewall policy, there is no change in work flow for publish and update. Therefore, both the zone based rules and global base rule are published and updated together.

The basic settings of a firewall policy are obtained from the policy profile. The basic settings include log options, firewall authentication schemes, and traffic redirection options.

Firewall policies are displayed in the Tabular view. The left pane of the Tabular view displays all firewall policies. The right pane of the Tabular view displays the rules for the firewall policy that is highlighted in the left pane.

## Rule Base Overview

Security Design allows you to configure one type or both types of rule bases for each policy. If devices are assigned to a policy that does not have one of the rule bases under its management, Security Design still interprets that rule base as being under its scope. For example, if you configure firewall policies out of band on a device under an unmanaged rule base, Security Design deletes those policies. If you do not select the previously

configured rule base in a policy in the Security Design policy modify workflow, Security Design automatically deletes all rules in the policy in the next publish and update.

### Example: UnManaging a Previously Managed Rule Base

You can remove a managed device from the Security Design management scope. To unmanage a previously managed rule base when no other policies are published on the device except the existing policy:

1. Do not select the **Manage Global Policy** option on modifying a device policy in Security Design.
2. Security Design deletes the global rule base in the design data of the Security Design application.
3. Publish a policy and update the device. The update deletes all global rules from the device.
4. On successful update, the all devices policy for the device is removed from the Security Design management scope.



**NOTE:** Security Design will continue to delete any all devices policy configured on the device through the CLI at subsequent publish updates.

#### Related Documentation

- [Creating Firewall Policies on page 90](#)
- [Adding Rules to a Firewall Policy on page 107](#)
- [Ordering the Rules in a Firewall Policy on page 110](#)
- [Managing Firewall Policies on page 121](#)
- [Publishing Firewall Policies on page 111](#)

## Multiple Group Policy Membership Overview

The Multiple Group Policy Membership feature supports the placing of devices in more than one policy group, and assigning priorities to the policy groups. This way, the policies, and the rules within them, are applied in the desired order.

The group priority of firewall group policy has the following two parts:

- Priority
- Precedence

Priority indicates the order in which rules are pushed to the device. Priority can be set to high, medium, or low. Precedence is a value that controls the ordering of group policies within a priority level. If two policies are assigned the same priority, their precedences set the order in which the rules are pushed.

## General Rules About Priority and Precedence

When you create or edit a group policy, if you set the precedence to the same value as an existing policy, the newly created or modified policy gets the assigned precedence. The existing group policy that had the same precedence, and all lower priority (higher precedence value) policies, will have their precedence value increased by 1.

If you make changes to a policy, such as deleting policy, or moving a policy from a different priority level, Security Design reorders the precedence of all policies in that priority level.

### Example: New Precedence of a Policy Set to the Same Precedence as an Existing Policy

In this example, three medium-priority policies, PolicyA, PolicyB, and PolicyC, are assigned precedences 1, 2, and 3, respectively. If you create a new policy, PolicyNew, and set the priority to medium and the precedence to 2, the order of the policies changes to PolicyA, PolicyNew, PolicyB, and PolicyC, with precedence 1, 2, 3, and 4, respectively.

## Sorting of Firewall Policy Left Pane

The left pane of the firewall policies can be sorted based on priority or precedence values, alphabetically, and by creation or modification time. Global policies always appear at the top of the right pane, and device policies appear at the bottom of the right pane. Only group policies are sorted.

Figure 24: Sorting Order in the Firewall Policy Left Pane

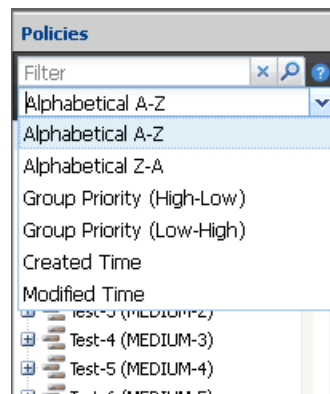


Table 3 on page 86 shows the different sorting orders available for firewall policies.

Table 3: Sorting Order for Firewall Policies

Sorting Order	Description
Alphabetical A-Z	Group policies are sorted alphabetically in ascending order.
Alphabetical A-Z	Group policies are sorted alphabetically in descending order.
Group Priority (High-Low)	Group policies are sorted in the order High, Medium, and Low. For the same priorities, the lower precedence number is placed in the top. For example, High 1 has higher precedence than High 2.



Table 3: Sorting Order for Firewall Policies (*continued*)

Sorting Order	Description
Group Priority (Low-High)	Group policies are sorted in the order Low, Medium, and High. For the same priorities, the higher precedence number is placed in the top. For example, Low 3 has lower precedence than Low 2.
Created Time	Policies are listed based on creation time. The policy created first is placed at the top.
Modified Time	Last modified policies are placed at the bottom (last).



**NOTE:** You cannot set the precedence value greater than the available precedence values that are assigned to the available priority policies. Based on the priority of the policies, the precedence values are applied.

To hide the policies in the left pane that do not have any defined rules:

1. At the bottom of the left pane, click the expandable **Policy View Settings** option.
2. Click the **Hide Empty Device Policies** check box to hide the device exception policies that do not have any rules. Clicking the check box will only hide those device exception policies inside group policies which do not have any rules, not the empty standalone device policies.

#### Related Documentation

- [Managing Firewall Policies on page 121](#)
- [Policy Priority Precedence Setting on page 103](#)
- [Publishing Firewall Policies on page 111](#)

## Global Address Book Overview

In Junos OS Release 11.2 and later releases, the address book is moved from the zone level to the device global level. This permits objects to be used across many zones and avoids inefficient use of resources. This change also permits nested groups to be configured within the address book, removing redundancy from repeating address objects.

The Security Design application manages its address book at the global level, assigning objects to devices that are required to create policies. If the device is capable of using global address book, Security Design pushes address objects used in the policies to the device global address book. Nested address group capability is used in the publish and update feature of Security Design depending on the device capability.

## Differences Between Global and Zone-Based Address Books

The global address book is supported in Junos OS Release 11.2 and later releases.

- An address book is not configured within a specific zone; therefore, one address book can be associated with multiple zones.
- If a global address book is defined, you cannot create zone-based address books.
- By default, there is an address book called *global* associated with all zones.
- A zone can be attached to only one address book in addition to the global address book, which contains all zones by default.
- Address name overlaps are possible between the global address book and zone address book. For example, Security Design will attempt to match an address in the zone-based address book first, and, if the address is not found, the global address book is checked. You must ensure that the correct address objects are used in the policy.
- NAT rules can use address objects only from the global address book. They cannot use addresses from user-defined address books.



**NOTE:** Beginning in Junos OS Release 12.1, zone-based address books are no longer supported. Devices running Junos OS Release 12.1 or later must use the global address book.

---



**NOTE:** Beginning in Junos OS Release 11.2, NAT rules can use address objects from the global address book. However, Security Design will still continue to define the NAT address in the rule itself rather than referring to the global address book.

---

## Nested Address Group Support

In Junos OS versions before Release 11.2, nested address groups were not supported on the device. Because of this, address groups were flattened to a single group when pushed to the device. This caused inefficient of object resource usage. Junos OS Release 11.2 and later releases support the nested references within address sets.

## Mixed-Version Support

Because Security Design supports Junos OS Release 10.3 and later releases, support for both zone-based and global address books is required. SRX Series devices running Junos OS Releases earlier than Release 11.2 must support the current behavior, that is, populating required address book entries in the zone address books and flattening nested groups. SRX Series devices running Junos OS Release 11.2 and later must use the global address book.

Junos OS Release 11.2 supports both zone address and global address books. However, both are configured separately.

## Migrating from Zone to Global Addressing

Table 4 on page 89 gives the migration matrix covering all scenarios:

**Table 4: Migration Matrix**

Address Book Used in Last Push from Security Design or NSM	Is Device Global Address Book Capable?	Address Book Type Used by Device	Security Device That Will Use Zone or Global
Zone	NA	Zone	Zone
Zone	NA	Global	Global
Zone	Any	Empty	Depends on device capability
Empty	Yes	NA	Global
Empty	No	NA	Zone



**NOTE:** In Junos OS Release 11.2 and later releases, devices might be managed by the Security Design and the device might be using zone address book. In this case, if you want to use global address book, you can do offline device migration from zone address book to global address book. In this case, if the device was managed by the Security Design application, user must publish the device again, so that the changes are discovered by the application.

- Related Documentation**
- [Firewall Policies Overview on page 83](#)
  - [Creating Firewall Policies on page 90](#)
  - [Managing Firewall Policies on page 121](#)

## Creating Firewall Policies

---

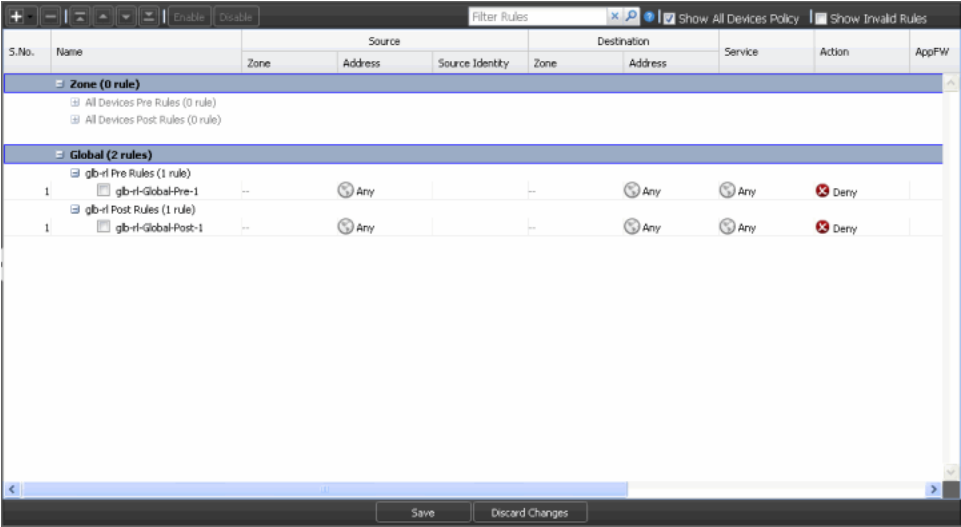
To create a firewall policy:

- 1. From the **Security Design** task ribbon, select **Firewall Policy** .

The Policy Tabular view appears. The Policy Tabular view is a table with two panes. The left pane displays all the firewall policies in the system, which includes device, group, and global firewall policies.

If you click a firewall policy in the left pane, the right pane displays the rules and rule groups for the respective policy, as shown in [Figure 25 on page 91](#).

Figure 25: Firewall Policy Tabular View



The right pane of the of firewall policy ILP divides the two rule bases. All zone-based rules are grouped under **Zone**, and the SRX all devices rules are grouped under **Global**. You cannot move a rule from one section to the other. The same set of features are available to both the rule bases, however.



**NOTE:** While adding rules, you can select to add them either to the zone rule base or to the global rule base.

You can search for firewall policies in the left pane using the firewall policy names and devices that are used in the firewall policy. You can search rule in the right pane using zones, addresses, description, and services used in the rule.

On the right pane, you can search for rule by using specific search tags, as shown in the [Table 5 on page 91](#)

Table 5: Firewall policy Right Page Search Options

Rule Column	Search Tag	Example Usage	Expected Behavior
Source address name	dcRuleSrcAddressName	dcRuleSrcAddressName:ServerFarm	Searches rules which has serverFarm as source address
Source address IP	dcRuleSrcIPAddress	dcRuleSrcIPAddress:1.1.1.1	Searches rules which has an address with ip 1.1.1.1 in source address

Table 5: Firewall policy Right Page Search Options (*continued*)

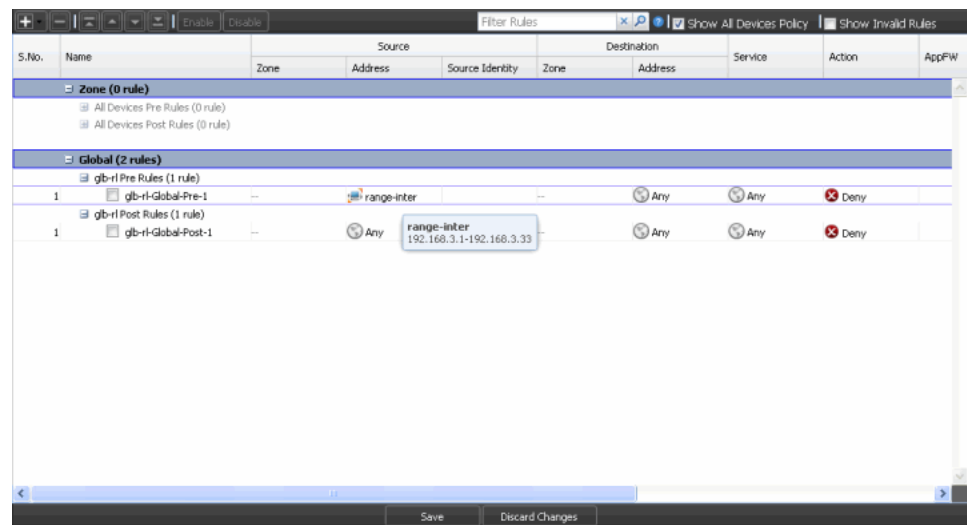
Rule Column	Search Tag	Example Usage	Expected Behavior
Destination address name	dcRuleDstAddressName	dcRuleDstAddressName:ClientMachine	Searches rules which has ClientMachine as destination address
Destination address IP	dcRuleDstIPAddress	dcRuleDstIPAddress:1.1.1.1	Searches rules which has an address with IP 1.1.1.1 in destination address
Application name	dcRuleAppName	dcRuleAppName:ftp	Searches rules with application ftp
Application source port	srcPort	srcPort:11243	Searches rules using application with source port 11243
Application destination Port	dstPort	dstPort:22	Searches rules using application with destination port 22
From Zone	dcRuleFromZone	dcRuleFromZone:trust	Searches rules whose from zone is trust
To Zone	dcRuleToZone	dcRuleToZone:untrust AND dcRuleFromZone:trust	Search Rules whose from zone is trust and to zone is untrust



**NOTE:** Any changes you make to both the zone and SRX all devices rule bases are saved or discarded together as a single change list.

You can use the available Tooltip view to see information about policy objects. To see the tooltip for an object, move the mouse over its source or destination address for which details are required. The tooltip displays the address name and other address object details (IP and subnet), as shown in [Figure 26 on page 93](#). For address group, the tooltip shows details regarding its members.

Figure 26: Tooltip Showing Object Information



Tooltips are also available for services. Mouse over a service group to view the group name and other information such as protocol and destination port. For a service group, member details are shown in the tooltip.

2. Click **Create Policy** from the task ribbon.

The **Create Policy** page appears. You can create a group policy or a device policy on this page.

3. Create a group policy:

- a. Enter the name of the group policy in the **Name** field.
- b. Enter a description for the group policy rules in the **Description** field. Security Design sends the comments entered in this field to the device.
- c. By default, the **Manage Zone Policy** option is selected and used to manage zone-based firewall rules.
- d. Select **Manage Global Policy** to manage the global firewall rules for SRX Series devices.

You can select either one or both options. Security Design does not allow you to unselect both options.

- e. To set the priority for a policy, select **High**, **Medium**, or **Low** from the **Priority** list.
- f. Enter a **Precedence** value less the number of existing policies of the same priority. The number of existing policies are displayed as part of the **Precedence** field.

For example, if the system has 4 policies Low priority, 5 policies with Medium priority, and 3 policies with High priority, you can set the precedences as follows:

- Low-priority policies—1 through 4
- Medium-priority policies—1 through 5

- High-priority policies—1 through 3
- g. Select the profile for the group policy from the **Profile** menu.
  - h. Select the IPS mode from the **IPS Configuration Mode** menu.
  - i. Click the **Show Assigned Devices** check box to make the devices on which policies have been configured available for selection.
  - j. Select the devices on which the group policy will be published, in the **Select Devices** pane, select the devices from the **Available** column and click the right arrow to move these devices to the **Selected** column.

You can also search for devices by entering the device name, device IP address, or device tags in the **Search** field in the **Select Devices** pane. Once the searched devices appear, you can move them to the **Selected** pane, as shown in [Figure 27 on page 94](#).

**Figure 27: Create Firewall Policy**

By default, all devices appear under **Select Devices** tab whether or not they have been assigned to an all devices policy. To see which devices are unassigned, select the **Show devices without existing policy** option to see the devices that are not assigned to an all devices policy.

- k. Click **Create**.





**NOTE:** One device can hold configuration data related to one firewall policy only. Hence you cannot share devices for multiple firewall policies.

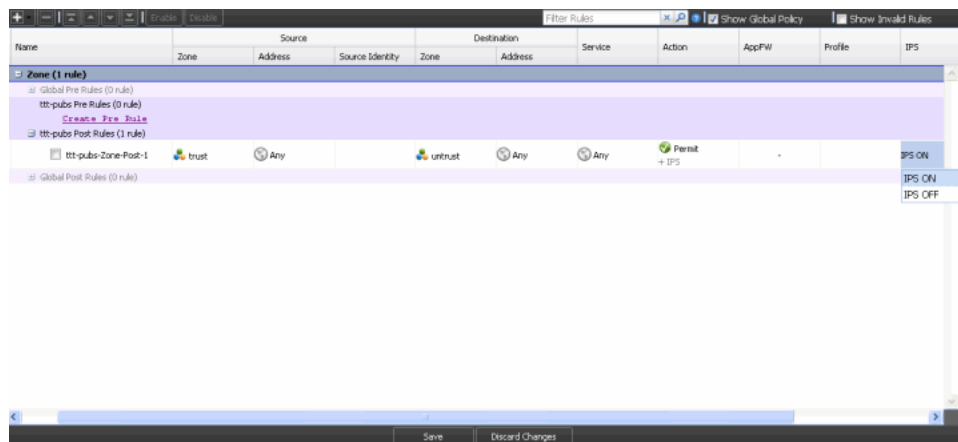
4. Create a device policy:
  - a. Enter the name of the device policy in the **Name** field.
  - b. Enter a description for the device policy in the **Description** field.
  - c. Select the profile for the device policy, from the **Profile** list.
  - d. Select the IPS mode from the **IPS Configuration Mode** list. The following [Table 6 on page 95](#) shows different IPS configuration modes and the purpose:

**Table 6: IPS Configuration Mode**

IPS Mode	Description
Basic	To turn IPS on or off. The recommended signature set is used for the policy.
Express	To select IPS only from the predefined and custom signature set. You can select different signature set.
Manual	To turn IPS on or off with the ability to customize the IPS policy. An empty container for this IPS policy is created in the IPS Management workspace. You must manually add the IPS policy rules for these IPS policies. You can add more IPS policy rules manually.

You can turn the IPS policy on or off by double-click on the IPS column, as shown in the [Figure 28 on page 95](#).

**Figure 28: Turning an IPS Policy on or off**



If you have set the IPS policy to ON, an empty container is created in the IPS management workspace for the same global, group, or device policies.

All these IPS modes are available for logical systems also.

- e. Select the device on which the device policy will be published from the **Device** list.
- f. Click **Create**.



.....

**NOTE:** When you are viewing a group policy, if you do not want the all devices policy rules to appear in the Policy Tabular view, uncheck the clear the **Show Global Policies** check box in the right pane. When you are viewing a device policy, if you do not want the global and group policy rules to appear in the Policy Tabular view, clear the **Show Global/Group Policies** check box in the right pane.

.....



.....

**NOTE:** You can use the search boxes in the left pane and right pane to search for firewall policies and the rules in a specific firewall policy, respectively.

.....



.....

**NOTE:** SRX Series logical systems support complete firewall policy configuration in Security Design. The captive portal is configured in the root logical system and referred from the user logical system. If IPS policy is assigned to a logical system, it enables only the basic IPS mode. When the logical system is published, you'll received a warning message that the logical system shares only the root device configuration.

.....

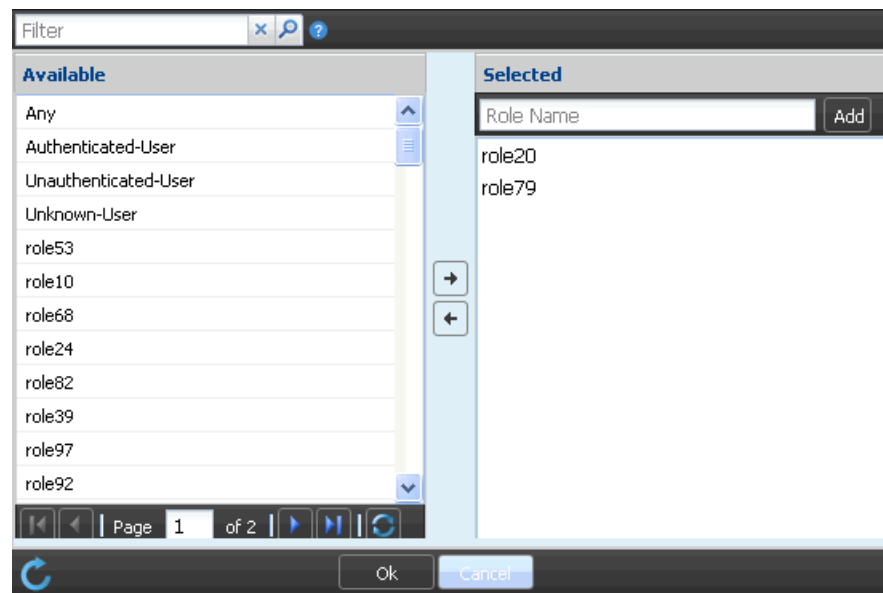
The Infranet Controller (IC) maps users to roles based on the information provided by an authentication server. For example, a user could be mapped to a role based on membership in Active Directory groups.

When a user attempts to access a resource, SRX Series device passes the username and password to the IC. The IC responds with the role(s) that you are mapped to. The SRX Series device then evaluates the security policies to determine whether the user can access the resource.

To add a role to a user:

1. Click on **Source Identity** in the source identity table header. A window appears, as shown in [Figure 29 on page 97](#).

Figure 29: Source Identity Page



In addition to the roles provided by IC, the following roles are valid:

- Free text—You can enter a new role name and click **Add** in the right pane.
  - Any—Default role that matches with any user. The Any role cannot be used in any rule that uses other types of roles. Ensure that the text you enter matches with a role configured in IC.
  - Authenticated-User—User who has an entry in any of the user identification tables (local or ICs). The Authenticated-User role cannot be used in any rule that uses other types of roles. An authenticated user is sometimes referred to as a *known user* in other firewalls.
  - Unauthenticated-User—User with an IP address that does not match the available IP addresses in the user authentication table of the SRX Series device.
  - Unknown-User—Authorization service is unavailable for this user.
2. Click the redo icon to select devices for the selected roles. The following window appears for selecting the devices, as shown in [Figure 30 on page 98](#).

Figure 30: Select Devices Page

The screenshot shows a window titled "Select Devices to obtain Local Auth and IC table". Inside, there is a "Filter" input field with a search icon. Below this are two columns: "Available" and "Selected". The "Available" column contains the text "fib". Between the columns are two arrow buttons (right and left). At the bottom of the window are "Ok" and "Cancel" buttons.

Security Design maintains a list of roles available for a group or for individual devices. You can manually retrieve the available roles from a single SRX Series device or from multiple SRX Series devices.



**NOTE:** Every time you perform a role retrieval, the existing list is overwritten. This prevents deleted roles from persisting.



**NOTE:** Because you are manually retrieving roles from the SRX Series devices, Security Design might not recognize a valid role on an SRX Series device until you manually retrieve that role.

#### Related Documentation

- [Firewall Policies Overview on page 83](#)
- [Adding Rules to a Firewall Policy on page 107](#)
- [Ordering the Rules in a Firewall Policy on page 110](#)
- [Managing Firewall Policies on page 121](#)
- [Publishing Firewall Policies on page 111](#)

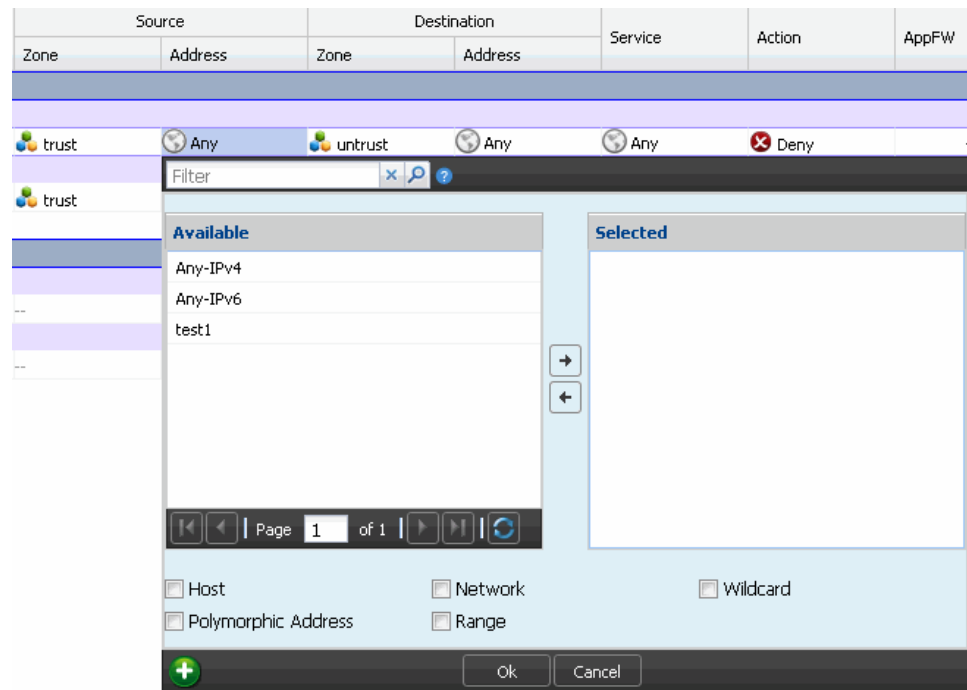
## Inline Creation of Objects in Policy

To optimize the creation of policies, Security Design allows you to create new objects for policies you create with the policy editor.

To create objects for a source address:

1. In the all devices policy page, click on the source address column. [Figure 31 on page 99](#) shows the window that appears showing the available addresses and options for creating the new object.

**Figure 31: Inline Address Object Creation in the Source Address Window**



2. Click the plus sign (+) to create the new address object.

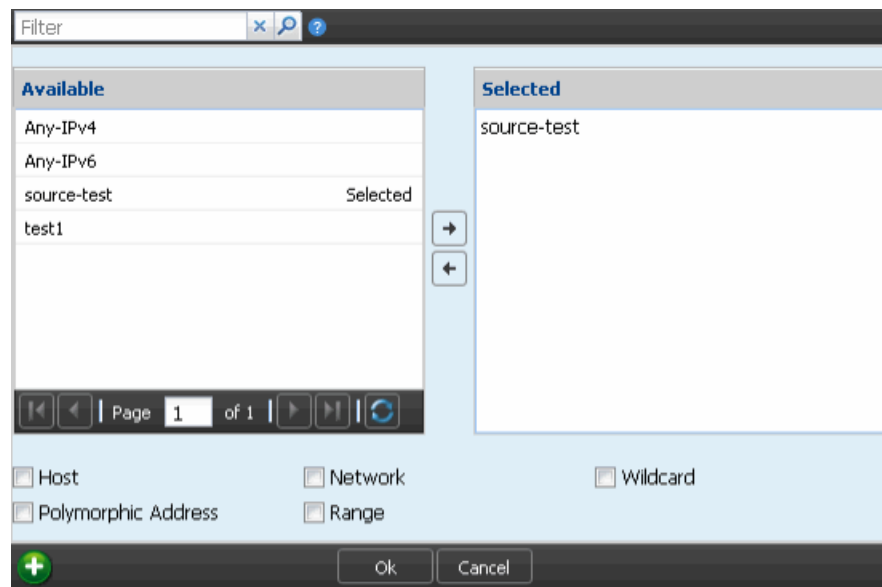
[Figure 32 on page 99](#) shows the page that appears.

**Figure 32: Inline Address Object Create Page**

The **Type** can be Host, Range, or Network.

3. Click **Create** to finish editing the object. This adds the newly created address object to the selected addresses and returns to the address selector.

Figure 33: Address Selector Page Showing the New Inline Object



4. Click **Cancel** to discard your changes and return to the address selector.

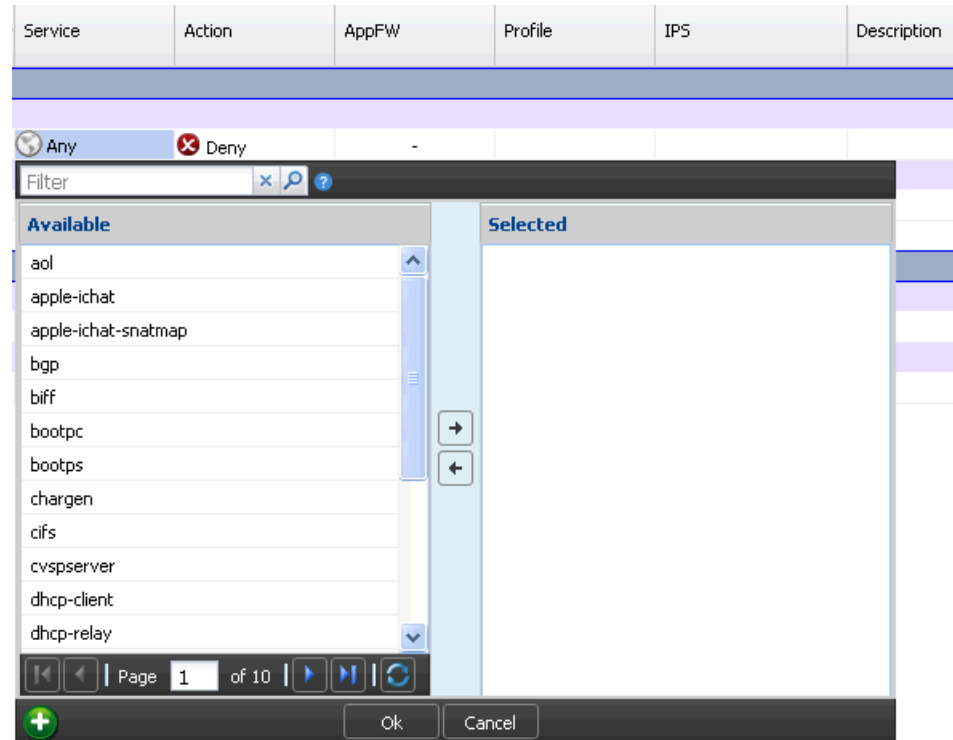


**NOTE:** Follow the same steps to create objects for the destination address.

To create objects for a service:

1. Click on the service column. Figure 34 on page 101 shows the window that appears, showing the available services.

Figure 34: Inline Service Object Creation in the Service List



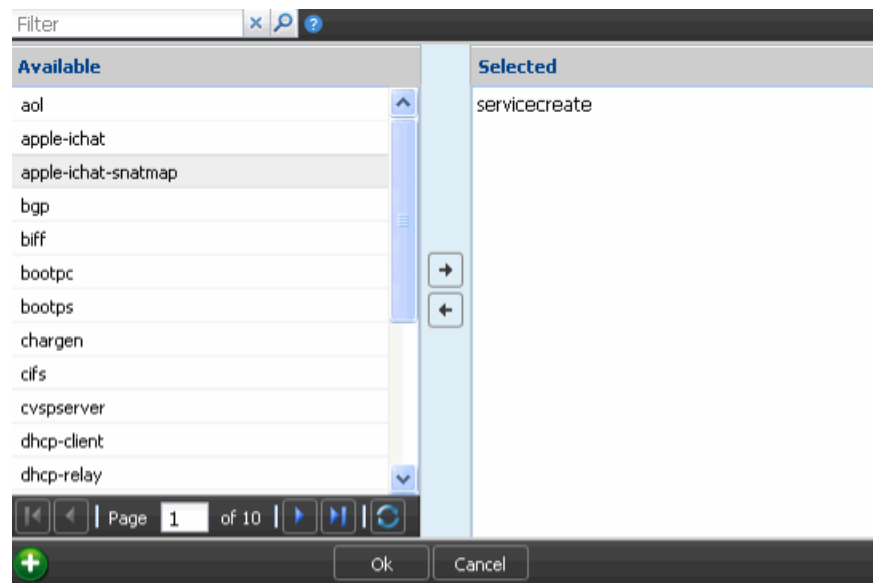
2. Click the plus sign (+) to create objects for the service.

Figure 35: Inline Service Object Creation Page

**Type** can be TCP or UDP. Any advanced options must be edited in the Object Builder workspace.

3. Click **Create** to finish editing the object. This adds the newly created object to the selected service and returns to the service selector.

Figure 36: Service Selector Page Showing the New Object



4. Click **Cancel** to discard your changes and return to the service selector.

**Related  
Documentation**

- [Firewall Policies Overview on page 83](#)
- [Managing Firewall Policies on page 121](#)



## Policy Priority Precedence Setting

---

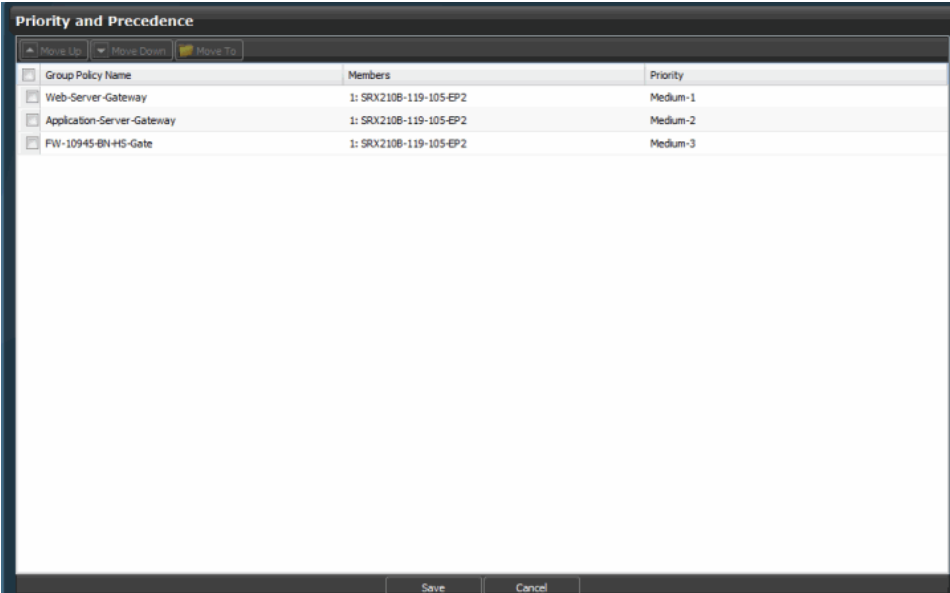
To change the priorities and precedences of different policies simultaneously:

1. From the **Security Design** taskbar, select **Firewall Policy > Policy Priority**.

The **Priority and Precedence** page appears with all the group policy names. The page contains the following fields:

- Group Policy Name—Name of the group policies.
- Members—Devices attached to the individual group policies. For example: 1:10.205.119.8 indicates that there is only one device attached to the group policy, and the device name or IP address is 10.205.119.8.
- Priority—Priority of the group policy (Low, Medium, or High).

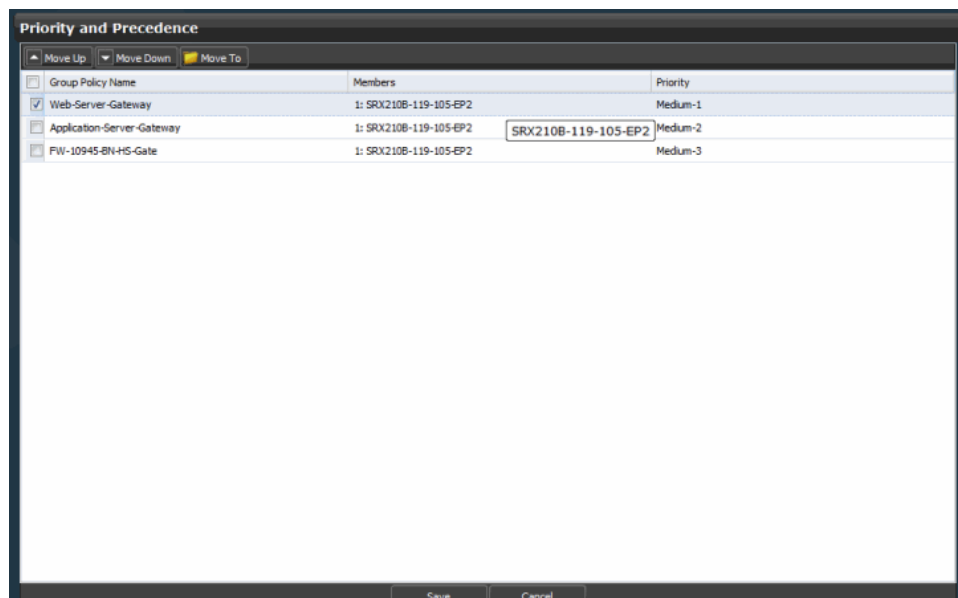
Figure 37: Policy: Priority And Precedence Page



Group Policy Name	Members	Priority
Web-Server-Gateway	1: SRX2108-119-105-EP2	Medium-1
Application-Server-Gateway	1: SRX2108-119-105-EP2	Medium-2
FW-10945-BN-HS-Gate	1: SRX2108-119-105-EP2	Medium-3

The tool tip is provided to list the number of devices attached to any group policy. Move the mouse over the Members column to get the tool tip, as shown in [Figure 38 on page 104](#).

Figure 38: Priority Precedence Tool Tip



2. Select any group policy and right click on the selected policy. The following options shown in [Table 7 on page 105](#) are provided to move the priority up or down or to change the precedence and priority simultaneously.

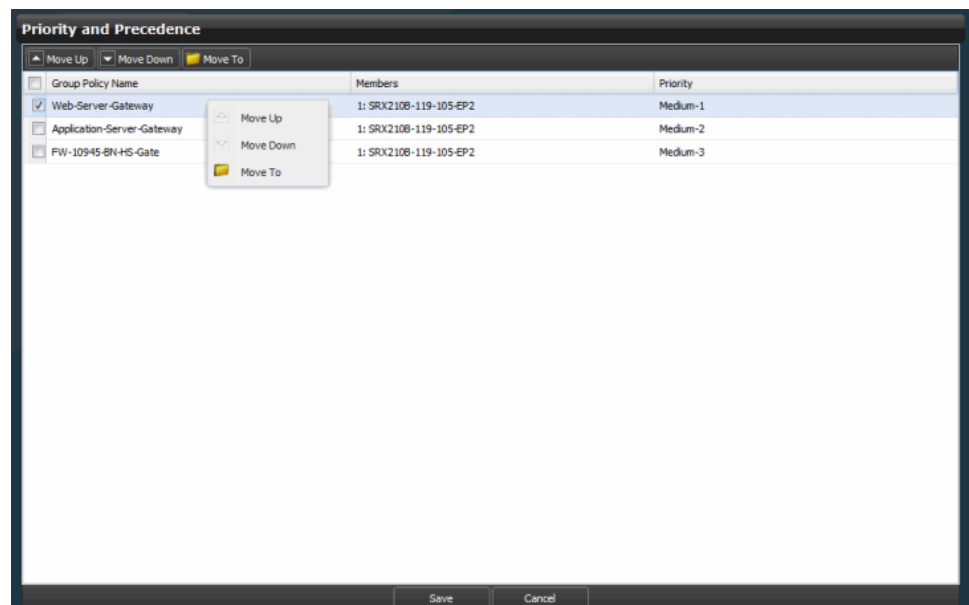
**Table 7: Priority and Precedence for Firewall Policies**

Options	Description
Move Up	<p>You can choose one or more polices and select the <b>Move Up</b> in the right-click menu. This option is also available in the tool bar. All the selected policies are moved up by one level. For example:</p> <ul style="list-style-type: none"> <li>• Move up a medium-priority policy with a precedence value 1. If a high-priority policy already exists, the Medium-priority policy is moved just below high-priority policy or move to high priority.</li> <li>• Move up a medium-priority policy with a precedence value 2. If a medium-priority policy with a precedence value 1 already exists, a medium-priority with precedence value 2 is moved up to precedence value 1 and an already existing medium-priority with a precedence value 1 is changed to precedence value 2.</li> <li>• Move up a low-priority policy with precedence value 1. The priority of the policy is changed to Medium with precedence value 1, only if there are no medium-priority policies, otherwise it would have the lowest precedence (highest number) in the medium- priority. If you move the policy up again, the priority of the policy is changed to High with precedence value 1.</li> </ul> <p>In all the Move Up operations, the remaining policies in the same priority are pushed up by one level.</p>
Move Down	<p>You can choose single policy or more than once policy and select the Move Down in the right click menu. This option is also available in the tool bar. All the selected policies are shifted by one level down individually. For example:</p> <ul style="list-style-type: none"> <li>• Move down medium-priority with precedence 1. If a medium-priority policy with precedence 2 exists, the precedence of the moved down policy becomes precedence 2, and the original precedence 2 policy is now precedence 1. If there are no other medium-priority policies, the move down moves the policy to low-priority and precedence 1.</li> </ul>

Table 7: Priority and Precedence for Firewall Policies (*continued*)

Options	Description
Move To	You can choose this option to set the priority and precedence at the same time. If you choose the same priorities for the policies, set the precedence value between 1 to number of policies of the same priority. If the priorities are different, set the precedence value between 1 to number of policies in the priority. If highest precedence medium priority policy is moved down, it becomes priority low and precedence 1.

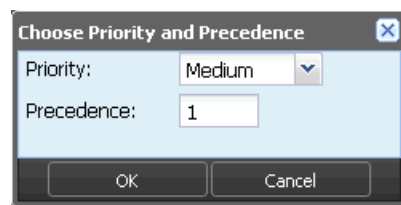
Figure 39: Priority And Precedence Right-Click Page



**NOTE:** If multiple policies are selected, all the policies are moved one-by-one to the given priority and precedence slot sequentially.

- Click on **Move To** to provide precedence value.

Figure 40: Setting Priority And Precedence Value Page



- Click on **Save** to save all the priority and precedence changes. These changes are saved in the database and page is shown with all the annotations of the changes. If you do not want to save, click on **Cancel** to go back to the firewall policies page.

- Related Documentation**
- [Multiple Group Policy Membership Overview on page 85](#)
  - [Managing Firewall Policies on page 121](#)

## Adding Rules to a Firewall Policy

When a new firewall policy is created, by default the policy displays links to create rules for the policy. If you have created a group firewall policy, you will see the **Create Pre Rule** and **Create Post Rule** link in the right pane. If you have created a device firewall policy, you will see the **Create Device Rule** link.

To add rules to a firewall policy:

1. From the **Security Design** task ribbon, select **Firewall Policy**.

The Policy Tabular view appears.

2. Click the security policy you want to add rules to from the left pane.

The existing rules of the security policy are displayed in the right pane.

3. Click the **Add Rule** icon and select the type of the rule you want to add.

A new rule is added in the bottom-most row of the Pre Rule, Post Rule, or Device Rule section, depending on the type of rule you have added. The rule is assigned a serial number based on the number of rules already added to the policy. By default, the Source zone is set to trust, Destination zone is set to untrust, and the Action is set to Deny. The Source address, Destination address, and Service is set to Any. You can now modify the default settings to the settings that you want for this security policy.

4. Click the **Name** field in the rule and change the name of the rule.
5. Click the **Source Zone** field in the rule and select the appropriate zone from the list of zones.

The zones that appear in the list are dependent on the type of security policy you have chosen to add rules to. If you are adding a rule for a group policy, all the zones present on all devices are available for selection. Select the correct zone for the device in the group policy.

6. Click the **Source Address** field in the rule.

The address selector appears.

7. Select the addresses you want to associate the rule to, from the **Available** column.
8. Click the right arrow in the address selector.

The selected addresses are now moved to the **Selected** column.

9. Click **OK**.

10. Click the **Destination Zone** field in the rule and select the appropriate zone from the list of zones.

11. Click the **Destination Address** field in the rule.

The address selector appears.

12. Select the addresses you want to associate the rule to, from the **Available** column.
13. Click the right arrow in the address selector.

The selected addresses are now moved to the **Selected** column.

- Click **OK**.
- Click the **Service** field in the rule.

The service selector appears.

16. Select the services you want to associate the rule to, from the **Available** column.
17. Click the right arrow in the service selector.

The selected services are now moved to the **Selected** column.

- Click **OK**.
- Click the **Action** field in the rule and select the appropriate action from the drop-down list of actions.

You can select Permit, Deny, Reject, or Tunnel as the actions.

If Tunnel action is selected, a list with all the policy based VPNs that are created is provided, as shown in [Figure 41 on page 108](#)

### Figure 41: Tunnel Option for Global Rule

Filter Rules										Show All Devices Policy	Show Invalid Rules
S.No.	Name	Source		Destination		Service	Action	AppFW	Profile		
	Zone	Address	Source Identity	Zone	Address						
Zone (40 rules)											
All Devices Pre Rules (10 rules)											
Device Rules (20 rules)											
1	Device-Zone-1	trust	Any	untrust	Any	Any	Tunnel (SRX220-b_tets)	-			
2	Device-Zone-2	trust	Any	untrust	Any	Any	Tunnel (SRX220-b_tets)	-			
3	Device-Zone-3	trust	Any	untrust	Any	Any	Deny	-			
4	Device-Zone-4	trust	Any	untrust	Any	Any	Deny	-			
test1 (7 rules)											
12	Device-Zone-5	trust	Any	untrust	Any	Any	Permit	-			
13	Grlp1-Zone-Pre-3	trust	Any	untrust	Any	Any	Deny	-			
14	Grlp1-Zone-Pre-4	trust	Any	untrust	Any	Any	Reject	-			
15	Grlp1-Zone-Pre-5	trust	Any	untrust	Any	Any	Tunnel	Select VPI...			
16	Grlp1-Zone-Pre-6	trust	Any	untrust	Any	Any	Deny	-			
17	Grlp1-Zone-Pre-7	trust	Any	untrust	Any	Any	Deny	-			
18	Grlp1-Zone-Pre-8	trust	Any	untrust	Any	Any	Tunnel (SRX220-b_tets)	-			
19	Device-Zone-6	trust	Any	untrust	Any	Any	Deny	-			
20	Device-Zone-14	trust	Any	untrust	Any	Any	Deny	-			

20. Click the **AppFW** field in the rule and select the appropriate AppFirewall settings from the **AppFW Configuration** window.



**NOTE:** You can modify the **AppFW** field only if the **Action** field in the firewall policy rule action is set to **Permit**.

21. Click the **Profile** field in the rule and select the appropriate profile.

You can either select a default profile, custom profile, or inherit policy profile from another policy. If you are selecting a custom profile, you can customize the options in the policy profile.

22. Click the **IPS** field in the rule and select the appropriate IPS mode.

The options available for selection will depend on the **IPS Configuration Mode** you have selected. [Table 8 on page 109](#) displays the options available based on the **IPS Configuration Mode**.

**Table 8: IPS Field Options**

IPS Configuration Mode	Options Available in the IPS Field
None	No options are available for selection and hence cannot be edited.
Basic	Options available are ON and OFF. Security Design uses recommended by default.
Express	Predefined and custom IPS signature-sets are available for selection.
Advanced	Predefined and custom IPS signature-sets are available for selection. IPS policy can also be created using the IPS signature-sets.



**NOTE:** You can modify the **IPS** field in the firewall policy rule only if IPS mode is set to Basic, or Advanced and the **Action** field is set to Permit.

23. Click the **Description** field and enter a description for the security policy.

24. Click **Save**.

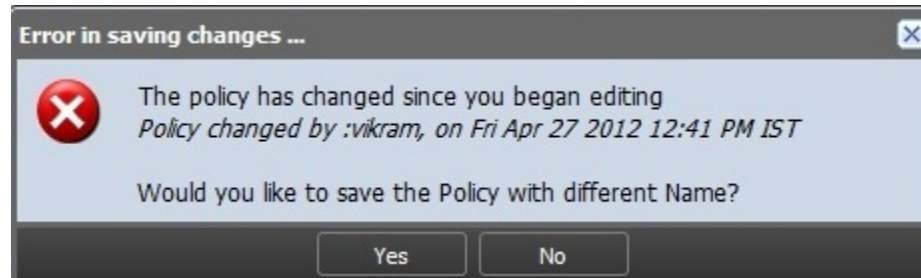


**NOTE:** You should click **Save** to save any changes you have made to the firewall policy. While in the process of making changes to the firewall policy, If you click on any of the tasks in the task ribbon before saving the firewall policy changes, all changes you have made will be lost. If you click anywhere inside the Policy Tabular view, a window appears, displaying a message asking if you want to confirm your changes.



**NOTE:** If a previous user has added new rules to the policy and saved the changes, when you attempt to save your changes, the error message shown in [Figure 42 on page 110](#) appears.

Figure 42: Concurrent Policy Edit Error Message



The error message shows the name of the user who made the previous changes and the time they were saved. The first user's changes take precedence over any later changes. You will be given an option to save the policy with a different name. Click **Yes** to save the policy with different name. Only saved rules are published to the policy.

#### Related Documentation

- [Firewall Policies Overview on page 83](#)
- [Creating Firewall Policies on page 90](#)
- [Ordering the Rules in a Firewall Policy on page 110](#)
- [Managing Firewall Policies on page 121](#)
- [Publishing Firewall Policies on page 111](#)

## Ordering the Rules in a Firewall Policy

To reorder the rules in a firewall policy:

1. From the **Security Design** task ribbon, select **Firewall Policy**.  
The Policy Tabular view appears.
2. Select the firewall policy whose rules you want to reorder.  
The rules of the firewall policy are displayed in the right pane.
3. Select a rule that you want to reorder and click the appropriate icon on the top of the right pane.

Icon Name	Description
Move Rule Up	Moves the rule one level up in the hierarchy.
Move Rule Down	Moves the rule one level down in the hierarchy.



Icon Name	Description
Move Rule to Top	Moves the rule to the top of the hierarchy.
Move Rule to Bottom	Moves the rule to the bottom of the hierarchy.

The rule is now positioned accordingly. When the policy is provisioned, the rules are provisioned to the devices in the order you have specified.

#### Related Documentation

- [Firewall Policies Overview on page 83](#)
- [Creating Firewall Policies on page 90](#)
- [Adding Rules to a Firewall Policy on page 107](#)
- [Managing Firewall Policies on page 121](#)
- [Publishing Firewall Policies on page 111](#)

## Publishing Firewall Policies

Publish considers priority and precedence values set on the policy and order rules on the device. Rules are published in the order of priority groups with Pre rules of High priority group publishing first before the pre rules of Medium and Low priority group. Within a same priority group, the Pre rules of policies with lower precedence value are published before the Pre rules of policy with higher precedence value. Device rules are published after all group Pre rules. This is followed by Group Post rules. The POST rules are published in the reverse order of Pre rules.

If you change the priority or precedence of a published policy, the policy must be republished for the changes to take effect. Sometimes, changing priority or precedence in one policy can affect other policies in the same priority group. However, such policies do not need to be republished in order for their changes in priority or precedence to take effect for the policies that are implicitly changed by the explicit changes to the republished policy.

To publish a firewall policy:

1. From the **Security Design** task ribbon, select **Firewall Policy > Publish policy**.

The **Services** page appears with all the firewall policies. It also displays the publish states of the firewall policies.

2. Select the check box next to the firewall policy that you want to publish.



**NOTE:** You can search for a specific device on which the policy is published by entering the search criteria in the search field, in the right top corner of the **Services** page. You can search the devices by their name, IP address, and device tags.



**NOTE:** If the firewall policy is to be published on a large number of devices, the devices are displayed across multiple pages. You can use the pagination and display options available on the lower ribbon, just below the list of devices to view all devices on which the firewall policy is published.

3. You can publish the IPS policies along with the firewall policies by selecting the **Include IPS Policy** check box. By default, this check box is selected.

If the **Include IPS Policy** check box is selected, two jobs are created after you click the **Publish** button. The first job is to publish the selected firewall policies. Once the firewall policy publish is successful, the IPS policy publish job is invoked.

If the **Include IPS Policy** check box is not selected, only the selected firewall policies are published.



**NOTE:** Firewall policy publish and IPS policy publish are mutually exclusive. The firewall policy publish job focuses only on firewall policy-related configuration, and IPS policy publish job focuses only on the IPS policy-related configuration.

4. Click the **Schedule at a later time** check box if you want to schedule and publish the configuration later, as shown in [Figure 43 on page 112](#).

**Figure 43: Policy Publish Page**

Name	Publish State	Description	Priority	Precedence
All Devices Policy	Not Published	Predefined Policy for all devices	-	-
gdb-t	Not Published		Medium	1
gdb-t-zn	Not Published		Medium	2

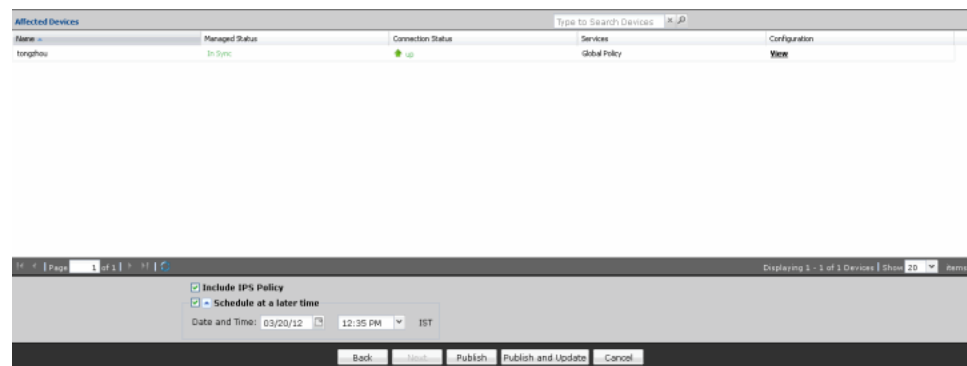
☒ Include IPS Policy  
☒ Schedule at a later time  
 Date and Time: 04/16/12 1:29 PM IST

Back Cancel Publish Publish and Update Cancel

5. Click **Next**.

The **Affected Devices** page displays the devices on which the policies will be published as shown in [Figure 44 on page 113](#).

Figure 44: Devices on Which the Policies Will Be Published



- If you want to preview the configuration changes that will be pushed to the device, click the **View** link in the **Configuration** column corresponding to the device. A **Configuration Preview** progress bar is shown while the configuration pushed to the device is generated.

The **CLI Configuration** tab appears by default. You can view the configuration details in the CLI format as shown in [Figure 45 on page 113](#).

Figure 45: Policy Publish: CLI Configuration



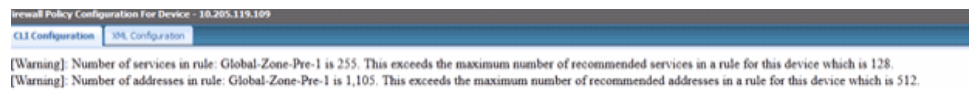
If the device does not support global policies, the rules are truncated with a warning message. A device will not support global policies for the following reasons:

- The device is running a Junos OS version earlier than 11.2.
- Global policy is supported only on the global address book. If the device is configured with a zone-based address book, Security Design will not publish a global policy for that device.

SRX Series devices have scaling capacity limitations for networking services. These capacities vary with the “platform” and Junos OS version. Security Design validates these limitations during the publish or preview of the policies and provides warning messages.

Security Design validates only the published service capacities. These validations are not applicable for the designed services that are still not published. If a particular capacity is exceeded, a warning message appears, as shown in [Figure 46 on page 114](#).

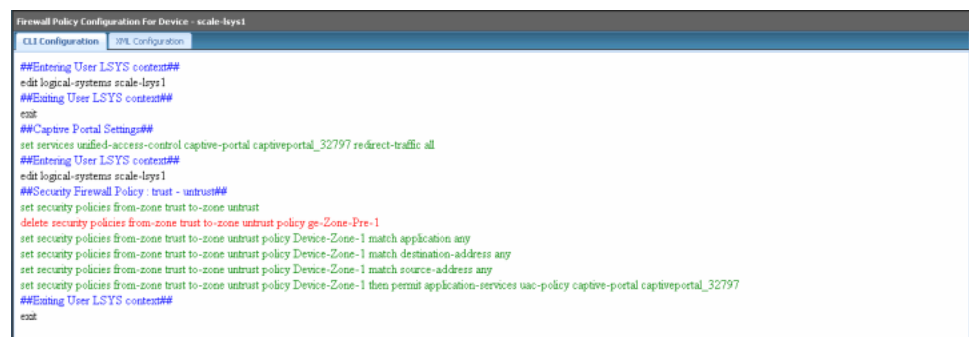
Figure 46: Device Validation Warning Message



For logical systems that have an assigned security profile, including the root logical system, Security Design validates the resource usage against the maximum and reserved quota configured in the respective profile.

If a logical system is assigned to services, you can publish those services to the logical system. You can view the configuration details in CLI format, as shown in [Figure 47 on page 114](#).

Figure 47: Policy Publish: LSYS Device CLI Configuration



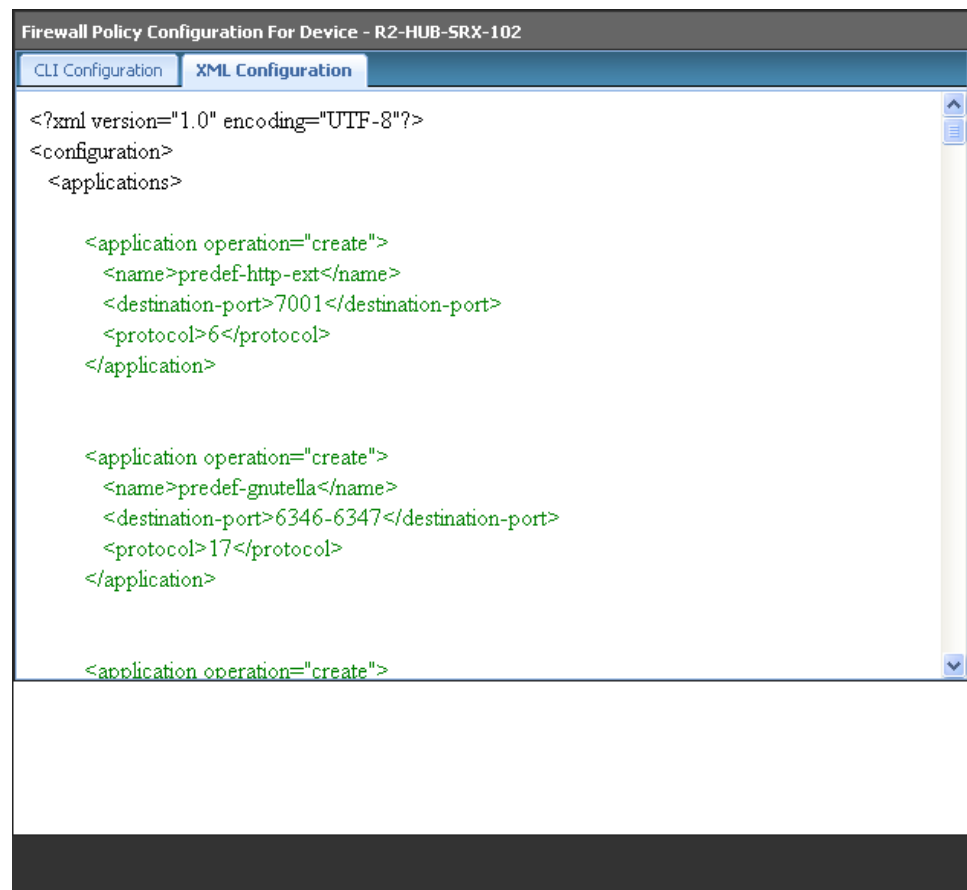
**NOTE:** Captive portal setting can be configured only at the root logical system and referenced only in the user logical system.



**NOTE:** Configurations update to the root logical systems are automatically done as part of the user logical system update. For such objects, the LSYS name is appended to the object names to differentiate across logical systems.

7. View the XML format of the configuration by clicking the **XML Configuration** tab, as shown in [Figure 48 on page 115](#).

Figure 48: Policy Publish: XML Configuration



8. Click **Back**.

9. Click **Publish** if you want only to publish the configuration.

A new job is created, and the job ID appears in the **Job Information** dialog box.

10. Click **Publish and Update** if you want to publish and update the devices with the configuration.

The firewall policy is now moved into the Published state if the configuration is published to all devices involved in the policy. If the configuration is not published to all devices involved in the firewall policy, the firewall policy is placed in the Partially Published state. If a firewall policy is created but not published, the firewall policy is placed in the Unpublished state. If any modifications are made to firewall policy configuration after it is published, the firewall policy is placed in the Republish Required state. You can view the states of the firewall policy by hovering over them.

A new job is created and the job ID appears in the **Job Information** dialog box.

11. Click the job ID to view more information about the job created. This action directs you to the **Job Management** work space.

If you get an error message during the publish or if the firewall policy publish fails, go to the Job Management workspace and view the relevant job ID to see why the publish failed.



**NOTE:** You can also publish a firewall policy by right-clicking the firewall policy in the Policy Tabular view and selecting **Publish Policy**. You are redirected to the **Affected Devices** page.



**NOTE:** You cannot publish a global firewall policy if you have not added rules to the all devices policy.



**NOTE:** During preview, the global rules shown under the comment Security Firewall Policy > Global, if global rules are supported. Otherwise, a warning message is shown.



**NOTE:** If you have configured AppFW and IPS for a firewall policy and the device you are using has the IPS license installed, when you publish and update the device with the firewall policy configuration, IPS and AppFW and IPS-related configuration will also be pushed to the device.



**NOTE:** When you publish a firewall policy that has a custom object associated to it, Security Design generates the custom object-related commands to be updated on the device. The commands for custom objects are generated irrespective of whether the firewall policy is already published or updated. If the custom object is associated with the firewall policy at the time of update, these commands are pushed to the device. Security Design pushes these commands to the device even though these commands may have been pushed to the device in an earlier update.

**Related  
Documentation**

- [Firewall Policies Overview on page 83](#)
- [Creating Firewall Policies on page 90](#)
- [Adding Rules to a Firewall Policy on page 107](#)
- [Ordering the Rules in a Firewall Policy on page 110](#)
- [Managing Firewall Policies on page 121](#)

## Custom Columns in Firewall Policy

- [Custom Column Overview on page 117](#)
- [Creating Custom Column Definitions on page 117](#)
- [Custom Column Data Search on page 118](#)
- [Managing Custom Column Definitions on page 119](#)

### Custom Column Overview

The Custom Column feature is a more structured mechanism used for various purposes such as for tracking changes to firewall policies, owner of the rule, by allowing you to define custom column views. Once the custom columns are defined, they appear on the right pane of the grid, similar to other columns. Data in these columns can be captured and saved in the same way as with other columns. You can also search the custom column data.

#### Related Documentation

- [Creating Custom Column Definitions on page 117](#)
- [Managing Custom Column Definitions on page 119](#)
- [Custom Column Data Search on page 118](#)

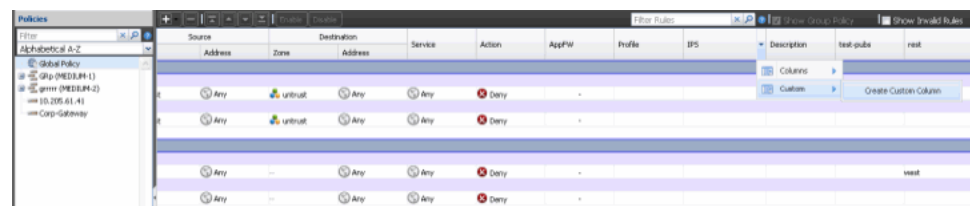
### Creating Custom Column Definitions

Custom columns are columns you define from the column header menu. Custom columns appear alongside other columns and apply to all policies in the system.

To create a custom columns definition for the firewall policy:

1. From the **Security Design** taskbar, select **Firewall Policy**.  
The Policy Tabular view appears.
2. Click on any field in the rule table header, select **Custom**, and then **Create Custom Columns**.

Figure 49: Creating Custom Column



3. A window appears. To create the custom column:
  - Enter the name of the custom column in the **Name** field. This is a mandatory field.
  - Enter the regular expression data in the **Validation Pattern** field to validate the entered data for the given custom column. For example, the typical e-mail regular expression looks like  
`^[A-Za-z0-9-]+(\.[A-Za-z0-9-]+)*@[A-Za-z0-9-]+(\.[A-Za-z0-9-]+)*(\.[A-Za-z]{2,})$`

This is an optional field. However, if you do not provide the regular expression data, the custom column data will not be validated.

**Figure 50: Creating Custom Column Page**



**NOTE:** The maximum number of custom columns you can define is 3.

4. Before creating the custom column, system will show the following warning message to confirm the custom column creation. Click **Yes** to create the custom column or **No** to cancel the custom column creation.

**Figure 51: Create Custom Column Confirm Page**

**Related Documentation**

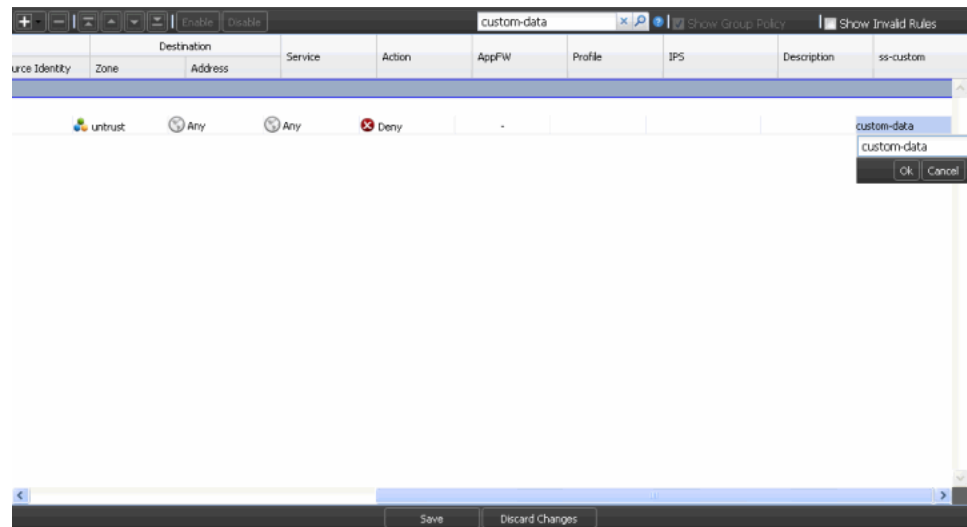
- [Custom Column Overview on page 117](#)
- [Custom Column Data Search on page 118](#)
- [Managing Custom Column Definitions on page 119](#)

## Custom Column Data Search

Once you entered or modified custom column data, you can perform searches on the data. Security Design searches for the data you specify within the custom column data you have created and filters the results by the rule name that matches the custom column name as well as by the custom column data.



Figure 52: Custom Column Data Search



#### Related Documentation

- [Custom Column Overview on page 117](#)
- [Creating Custom Column Definitions on page 117](#)
- [Managing Custom Column Definitions on page 119](#)

## Managing Custom Column Definitions

You can modify, delete, or export the custom column data.

- [Managing Custom Column Data on page 119](#)
- [Modifying Custom Columns Definitions on page 120](#)
- [Deleting a Custom Columns Definition on page 120](#)
- [Exporting a Custom Columns Definition on page 121](#)

### Managing Custom Column Data

You can insert, edit, or delete custom columns and their corresponding policy rules through an inline edit.

Security Design uses the following parameters to validate custom column data:

- Explicit regular expression—Validation is based on the optional regular expression property, if defined for the current custom column.
- Implicit length check—The maximum length of the data must be 256 characters. It is applicable to all custom columns.



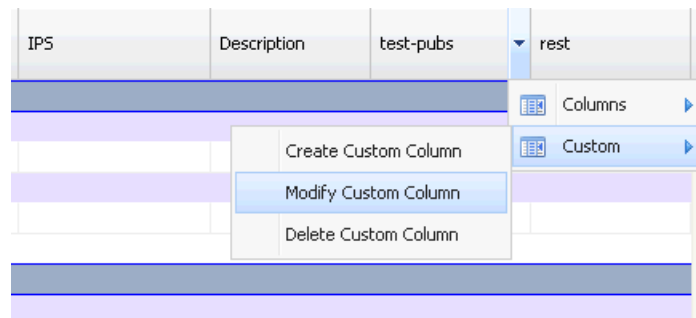
**NOTE:** The **Save** and **Discard** buttons which are used to save or discard all the edits—including inline edits of custom column fields—are not used for registering custom columns. These actions are committed as soon as they are completed in their respective UI and are independent of the **Save** or **Discard** button.

## Modifying Custom Columns Definitions

To modify a custom column:

1. Click the custom column name in the column header, go to **Custom**. Click and select **Modify Custom Column**.

Figure 53: Modifying a Custom Column



2. Once the edit is complete, the column header is refreshed to reflect the changes.



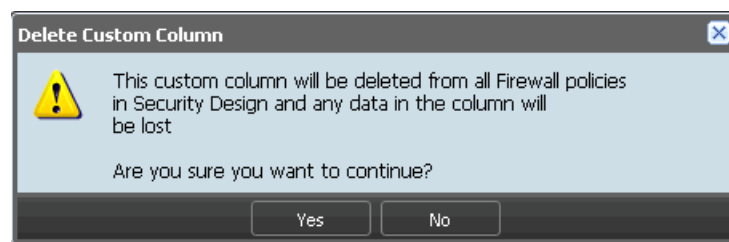
**NOTE:** You must have edit permissions to modify the custom column registration settings.

## Deleting a Custom Columns Definition

To delete the custom column definition:

1. Click on the custom column name in the column header, go to **Custom**, then select and click **Delete Custom Column**.
2. A delete confirmation message appears. After you confirm the deletion and the delete process finishes, Security Design updates the header and removes the column.

Figure 54: Deleting a Custom Column



### Exporting a Custom Columns Definition

---

Custom column definition is exported when a firewall rule is exported.

#### Related Documentation

- [Custom Column Overview on page 117](#)
- [Creating Custom Column Definitions on page 117](#)
- [Custom Column Data Search on page 118](#)

## Managing Firewall Policies

---

You can modify, delete, clone, or export security policies listed in the **Manage Policies** page.

To open the **Manage Policies** page:

- From the **Security Design** task ribbon, select **Firewall Policy**.  
The Policy Tabular view appears.

You can perform the following tasks in the **Manage Policies** space:

1. [Modifying Firewall Policies on page 121](#)
2. [Deleting Firewall Policies on page 122](#)
3. [Cloning Firewall Policies on page 123](#)
4. [Promoting a Firewall Policy on page 124](#)
5. [Exporting a Firewall Policy on page 124](#)
6. [Deleting Rules in a Firewall Policy on page 125](#)
7. [Cloning a Rule in a Firewall Policy on page 125](#)
8. [Grouping Rules in a Firewall Policy on page 125](#)
9. [Enabling/Disabling Rules in a Firewall Policy on page 126](#)
10. [Copying And Pasting Rules in Firewall Policy on page 126](#)
11. [Assigning Devices to a Firewall Policy on page 127](#)
12. [Deleting Devices from a Firewall Policy on page 127](#)

## Modifying Firewall Policies

To modify a firewall policy:

1. From the **Security Design** task ribbon, select **Firewall Policy**.  
The Policy Tabular view appears.
2. Right-click the security policy you want to modify from the left pane and select **Modify Policy**.

The **Edit Policy** window appears. You can modify the name, description, profile, and IPS configuration mode of the firewall policy.

Figure 55: Modify Policy Page

**Edit Policy**

Name:

Description:

☒ Manage Zone Policy [?](#)

☐ Manage Global Policy

Policy Priority:

Precedence:  2 ! Of 2

Profile:

IPS Configuration Mode:

3. You can modify the **Manage Zone Policy** and **Manage Global Policy** options.
4. You can modify the **Priority** and **Precedence** for the policy. If the priority is same or changed, you can enter precedence value from 1 to number of policies of the same priority. If the priority is changed, you can enter the precedence value from 1 to number of priorities.

For example, the system has 4 Low priorities, 5 Medium priorities, and 3 High priority policies. The following [Table 9 on page 122](#) shows the precedence value that can be set for different priorities.

Table 9: Setting Precedence Values for Different Priorities

Existing Priority	Modified Priority	Precedence that can be Set
Low	Low	1 to 4
Low	Medium	1 to 5
Low	High	1 to 4

5. Click **Modify**.

## Deleting Firewall Policies

To delete a firewall policy:

1. From the **Security Design** task ribbon, select **Firewall Policy**.  
The Policy Tabular view appears.
2. Right-click the firewall policy you want to delete and select **Delete Policy**.

A confirmation window appears.

3. Click **Yes**.



**NOTE:** If you delete a firewall policy, the erase configuration is sent to all devices that were a part of the firewall policy during the next **Update** operation for the device.



**NOTE:** If the published policy is deleted, Security Design application will unpublish the policy on the device.

## Cloning Firewall Policies

To clone a firewall policy:

1. From the **Security Design** task ribbon, select **Firewall Policy**.

The Policy Tabular view appears.

2. Right-click the firewall policy you want to clone and select **Clone Policy**.

The **Clone Policy** window appears. You can modify the name, description, profile, manage all devices policy, manage zone policy, priority, precedence, and IPS mode of the firewall policy. By default, the original policy values are displayed in the **Priority** and **Precedence** fields. If required, you can change them.

Figure 56: Clone Policy Page

The **Clone Policy** dialog box contains the following fields and controls:

- Name:** A text box containing the value "copy\_of\_Test-1".
- Description:** A large empty text area.
- Manage Zone Policy:** A checked checkbox with a help icon.
- Manage Global Policy:** An unchecked checkbox.
- Policy Priority:** A dropdown menu currently set to "Low".
- Precedence:** A text box containing the value "2", followed by a red warning icon and the text "Of 3".
- Profile:** A dropdown menu with the text "Select profile..." and a downward arrow.
- IPS Configuration Mode:** A dropdown menu with a help icon.
- Buttons:** "Clone" and "Cancel" buttons at the bottom.



**NOTE:** The priority and precedence value of the cloned policy is same as the priority and precedence of the original policy. For the other policies, the priority and precedence value will be moved to one level down.

3. Click **Clone**.

## Promoting a Firewall Policy

To promote a device policy to the group policy:

1. From the **Security Design** taskbar, select **Firewall Policy**.  
The Policy Tabular view appears.
2. Right-click the device policy you want to promote, and select **Promote Policy to Group Policy**.

The **Promote Device Policy to Group Policy** window appears, as shown in [Figure 57 on page 124](#).

**Figure 57: Promote Policy Page**

3. Enter the name, description, policy priority, and precedence. Click **Promote**.  
The device policy is promoted only to the prerule of the group policy.



**NOTE:** By default, the policy profile and IPS mode of a device policy is promoted to the group policy.

## Exporting a Firewall Policy

To export a firewall policy:

1. From the **Security Design** task ribbon, select **Firewall Policy**.

The Policy Tabular view appears.

2. Right-click the firewall policy you want to export and select **Export Policy**.

The **Export Policy** window appears.

3. Click **Export**.

## Deleting Rules in a Firewall Policy

To delete rules in a firewall policy:

1. From the **Security Design** task ribbon, select **Firewall Policy**.

The Policy Tabular view appears.

2. Select the firewall policy whose rules you want to delete.

The rules of the firewall policy appears in the right pane.

3. Select the check boxes next to the rules that you want to delete.

4. Click the **Delete Rule** icon on the top of the right pane.

## Cloning a Rule in a Firewall Policy

To clone a rule in a firewall policy:

1. From the **Security Design** task ribbon, select **Firewall Policy**.

The Policy Tabular view appears.

2. Select the firewall policy whose rule you want to clone.

The rules of the firewall policy appears in the right pane.

3. Select the check box next to the rule that you want to clone.

4. Right-click and select **Clone**.

## Grouping Rules in a Firewall Policy

To group rules in a firewall policy:

1. From the **Security Design** task ribbon, select **Firewall Policy**.

The Policy Tabular view appears.

2. Select the firewall policy whose rules you want to group.

The rules of the firewall policy are displayed in the right pane.

3. Select the check boxes next to the rules you want to group.

4. Right-click the rules and select **Rule Group > Create Rule Group**.

The **Create Rule Group** pop-up window appears.

5. Enter a name for the rule group in the **Name** field.

6. Enter a description for the rule group in the **Description** field.
7. Click **Create**.



**NOTE:** When the rule group is created, you can add rules in the rule group, modify the rule group name, move the rule into another rule group, ungroup rules, and ungroup rule groups using appropriate options.

---

## Enabling/Disabling Rules in a Firewall Policy

To enable or disable rules in a firewall policy:

1. From the **Security Design** task ribbon, select **Firewall Policy**.  
The Policy Tabular view appears.
2. Select the firewall policy whose rules you want to enable or disable.  
The rules of the firewall policy are displayed in the right pane.
3. Select the check boxes next to the rules that you want to enable or disable.
4. Click the **Enable** or **Disable** icon.



**NOTE:** You can enable or disable a rule group. When a rule group is disabled, all rules in the rule group are also disabled. The rule group row in the Tabular view is greyed out but the rules are not greyed out. However, the rules in the rule group are not published to the device during the publish operation, if they are disabled.

---

## Copying And Pasting Rules in Firewall Policy

To copy and paste rules in a Firewall policy:

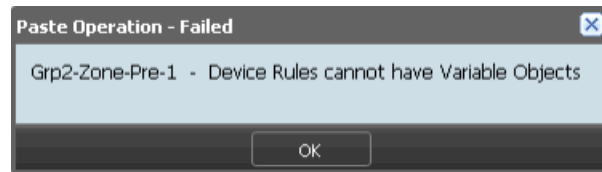
1. On the right pane, select the device rule that must be copied. Right-click on the selected device rule, and select **Copy**.
2. On the left pane, select the firewall policy that you want to paste the rule. On the right pane, right-click on the rule that you want the rule to be pasted. You can paste the rule before the selected rule or after the selected rule by choosing **Paste Before** or **Paste After** options.





**NOTE:** If you copy the rule having variable objects from the all devices policy and paste the rule in other policy rules, the following error message is received:

Figure 58: Variable Objects Rule Paste Error



## Assigning Devices to a Firewall Policy

To assign devices to a group firewall policy:

1. From the **Security Design** task ribbon, select **Firewall Policy**.  
The Policy Tabular view appears.
2. Right-click the firewall policy to which you want to assign devices and select **Assign Devices**.  
The **Assign Devices to Service** window appears.
3. Select the devices that need to be added to the firewall policy in the **Select Devices** pane, select the devices from the **Available** column and click the right arrow to move these devices to the **Selected** column.
4. Click **Modify**.

## Deleting Devices from a Firewall Policy

To delete devices from a group firewall policy:

1. From the **Security Design** task ribbon, select **Firewall Policy**.  
The Policy Tabular view appears.
2. Right-click the firewall policy from which you want to delete devices and select **Assign Devices**.  
The **Assign Devices to Service** window appears.
3. Select the devices that need to be deleted from the firewall policy in the **Select Devices** pane, select the devices from the **Selected** column and click the left arrow to move these devices to the **Available** column.
4. Click **Modify**.



**NOTE:** Deleting a device from a group firewall policy creates a device firewall policy. This policy carries all the device rules of the device from the group firewall policy.

**Related  
Documentation**

- [Firewall Policies Overview on page 83](#)
- [Creating Firewall Policies on page 90](#)
- [Adding Rules to a Firewall Policy on page 107](#)
- [Ordering the Rules in a Firewall Policy on page 110](#)
- [Publishing Firewall Policies on page 111](#)

## PART 5

# VPN

- [VPN on page 131](#)



## CHAPTER 16

# VPN

- [IPsec VPN Overview on page 131](#)
- [Creating IPsec VPNs on page 132](#)
- [Publishing IPsec VPNs on page 141](#)
- [Managing IPsec VPNs on page 143](#)

### IPsec VPN Overview

---

You can create site-to-site, hub-and-spoke, and full-mesh VPNs in the VPN Creation page. All VPNs in the system appear in the Tabular view. The left pane of the Tabular view displays the VPNs, and the right pane of the Tabular view displays the devices used for the respective VPN. If you want to use a custom VPN profile, you must configure a VPN profile before creating a VPN.

You can configure the following parameters for an IPsec VPN:

- Endpoints for a site-to-site VPN and full-mesh VPN
- Spokes and hubs for a hub-and-spoke VPN
- External Interface, Tunnel Zone, and Protected networks/zones for each device
- Routing settings
- VPN endpoint configuration

You can also customize endpoint-specific settings like VPN Name, IKE ID, and profile for each tunnel.

After the VPN configuration is saved, you can provision this VPN on the security devices.



**NOTE:** Security Design views each logical system as any other security device and takes ownership of the security configuration of the logical system. In Security Design, each logical system is managed as a unique security device.

Security Design ensures that the tunnel interfaces are exclusively assigned to the individual logical systems of a device. No tunnel interface is assigned to more than one logical system of the same device.



---

**NOTE:**

- IKE and IPsec security associations (SAs) must be configured at the root level for each VPN tunnel.
  - Only route-based VPNs are supported for the logical systems. Policy-based VPNs are not supported.
  - The assigned interface, *st0.x*, in one logical system must not overlap with other logical systems. However, multiple logical systems can be assigned with their own *st0* interfaces.
  - The *st0.0* interface must not be assigned to any logical system, because you cannot set up SA to this interface.
- 

In Security Design, route-based VPNs support OSPF, and RIP routing along with static routing. Static routing requires that the administrators specify the list of host or network addresses at each site is part of the VPN. For example, in a retail scenario, where thousands of spokes can be part of a VPN, the static routing approach generates a huge configuration at each device. Static routing requires the administrator to manually configure each route. Problems occur as the infrastructure changes or when the administrator does not have access to the addresses for the protected network. Keeping routes up-to-date manually creates tremendous overhead.

Security Design supports dynamic routing in VPN addressing. Security Design supports the dynamic routing protocols Open Shortest Path First (OSPF) and Routing Information Protocol (RIP). simplifies VPN address management by enabling the administrator to export static routes to a remote site over a tunnel, allowing the static route networks to participate in the VPN. However, only devices on the hub side can export static default routes to the device side. Devices at the spoke side cannot export static default routes over a tunnel.

If you select OSPF or RIP export, the OSPF or RIP network outside the VPN network are imported into VPN network through OSPF or RIP routing protocols.

**Related Documentation**

- [Creating IPsec VPNs on page 132](#)
- [Managing IPsec VPNs on page 143](#)
- [Publishing IPsec VPNs on page 141](#)

---

## Creating IPsec VPNs

---

1. [Creating IPsec VPNs on page 133](#)

## Creating IPsec VPNs

1. From the **Security Design** task ribbon, select **VPN > Create VPN**.

The VPN Tabular view appears, as shown in [Figure 59 on page 133](#).

**Figure 59: VPN Landing Page**

Device	External Interface	Tunnel Zone	Protected Zone/Networks	Route Settings	Routing Instance
SRX210-119-106	fe-0/0/4.0 (16.16.16.1)	VPN	Zones trust	Not Applicable	
SRX240B-108	fe-0/0/6.0 (4.4.4.2)	VPN	Zones trust-vpn	Not Applicable	VPN-Test
VPN-hsys-1 (10.205.61.42)	ge-0/0/6.0 (192.169.1.1)	VPN	Zones untrust-hsys1	Metric: 0	VR-LSYS140N

2. From the taskbar, select the **Create VPN** icon.
- The **Create VPN** page appears.
3. In the **Name** field, enter a name for the new VPN.
  4. In the **Description** field, enter a description for the new VPN.
  5. Select the **Tunnel Mode** as either **Route Based** or **Policy Based**.
  6. If you have selected **Route Based**:
    - a. Select the option button next to the type of VPN you want to create.
    - b. Select the VPN profile from the **VPN Profile** menu.



**NOTE:** If you choose to create a full-mesh VPN, you can choose only **Main mode profile** as the VPN profile.

- c. Select the option button next to the type of preshared key you want to use.
  1. If you select **Autogenerate** as the option for preshared key, select the **Generate Unique key per tunnel** check box to generate a unique key per tunnel, as shown in [Figure 60 on page 134](#).

Figure 60: Create VPN Page—Route-Based VPN

**Create VPN**

Name:

Description:

Tunnel Mode: ☒ Route Based ☐ Policy Based

Type: ☒ Site To Site ☐ Full Mesh ☐ Hub And Spoke

VPN Profile:

Preshared Key: ☒ Auto-generate ☐ Manual

☒ Generate Unique key per tunnel

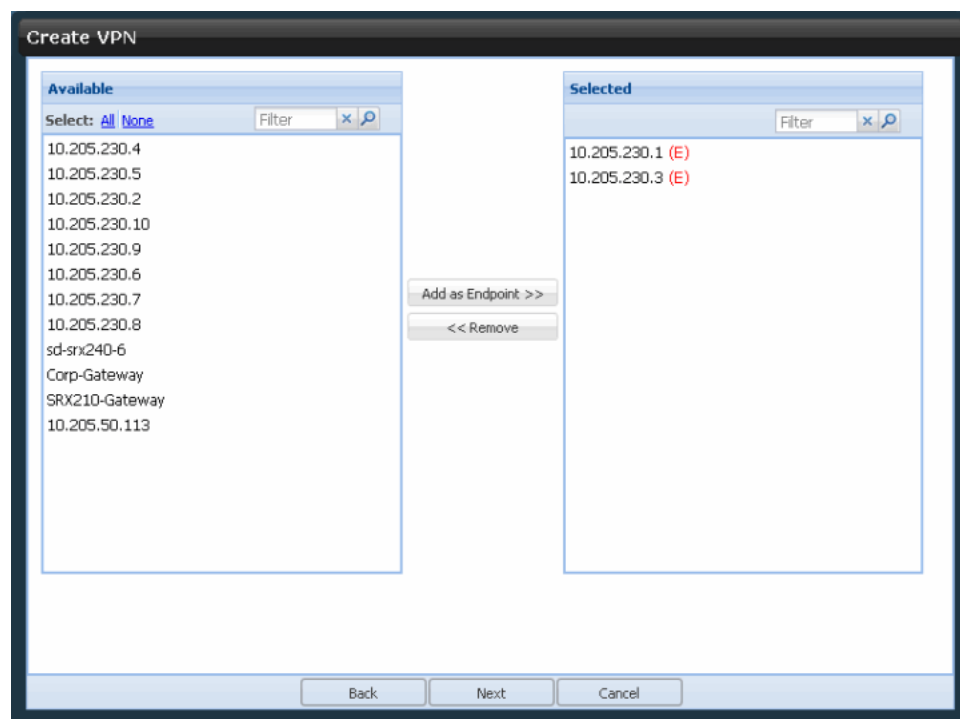
Back Next Cancel

2. If you select **Manual** as the option for the preshared key, enter the manual key in the **Manual Key** field.
- d. Click **Next**.

This page displays the **Available** and **Selected** panes.
- e. Select the device from the **Available** column, and click **Add as Endpoint**, as shown in [Figure 61 on page 135](#).



Figure 61: Create VPN: Add as Endpoint Page



- f. Click **Next**.
- g. Select the interface type in the **Tunnel Settings** pane.
  - If you select **Numbered** as the Tunnel setting, enter the IP subnet in the **IP Subnet** field.
  - Select the appropriate option button to choose the number of peers per tunnel interface.
  - If you choose **Specify Values**, enter the values in the **Specify Values** field, as shown in [Figure 62 on page 136](#).

Figure 62: Create VPN—Tunnel, Route, and Global Setting Pane

**Create VPN**

**Tunnel Settings**  
Interface Type: ☒ Unnumbered ☐ Numbered

**Route Settings**  
Routing Options: ☐ Static Routing ☒ OSPF ☐ No Routing ☐ RIP  
☐ Export Static Routes ☐ Export RIP Routes  
Area:

**Global Settings**  
Please select default values to be used for all devices in VPN.  
Per-device settings can be modified in the next step.

Type	External Interface	Tunnel Zone	Protected Network Zone
EndPoint			

Back Next Cancel

h. Select the routing option in the **Routing options** pane. If you select **OSPF**, the following check boxes are available:

- Export Static Routes—To export static routes.
- Export RIP Routes—To export RIP routes.
- Area—Numeric field where you enter the area ID.

If you select **RIP**, the following check boxes are available:

- Export Static Routes—To export static routes.
- Export OSPF Routes—To export OSPF routes.

i. In the **Global Settings** pane, under **Endpoint Configurations**, enter the external interface in the **External Interface** field.

j. In the **Global Settings** pane, under **Endpoint Configurations**, enter the tunnel zone in the **Tunnel Zone** field.

k. In the **Global Settings** pane, under **Endpoint Configurations**, enter the zone type in the **Protected Network Zone** field.

If you have chosen to create a hub-and-spoke VPN, you will see **Hub Configuration** and **Spoke Configuration**. Enter the appropriate values in the **External Interface**, **Tunnel Zone**, and **Protected Network Zone** fields in these panes.

l. If you have selected **Static Routing**, enter the values in the **External Interface**, **Tunnel Zone**, and **Protected Network Zone** fields for the type **Endpoint**.



**NOTE:** You can configure the custom routing instance for every device level, as shown in [Figure 63 on page 137](#). This is an optional field and by default, this field is blank. This option is available only for the static routing.

The **Global Settings** pane does not have an option to select the routing instance. You must manually select the routing instance for each endpoint in the tabular view.

Figure 63: Create VPN Page Showing Custom Routing Instance Option

Device	External Interface	Tunnel Zone	Protected Zone/Networks	Routing Instance
SRX210-119-106	ge-0/0/0.0 (10.205.119.106)	VPN	Zones trust	trust-VR
SRX240B-108	ge-0/0/0.0 (10.205.119.108)	trust	Zones trust	VPN-Test

m. If you have selected **No Routing**, enter the external interface in the **External Interface** field, and tunnel zone in the **Tunnel Zone** field for the type **Endpoint**.

n. Click **Next**.

The page that appears gives you a preview of the values you entered for the VPN, as shown in [Figure 64 on page 138](#). The page displays error indicators if the options you have configured do not map to the device. You can also click the **Show all Errors** check box to view all errors in the configuration. If errors are present, you must modify the configuration to eliminate them before you can proceed to the next step.

Figure 64: Create VPN—Route-Based VPN Preview

Device	External Interface	Tunnel Zone	Protected Zones	Route Settings
Amsterdam-106-PR01-Gateway	fe-0/0/5.0 (10.10.30.3)	vpn	Zones trust	Exported Routes: Static, OSPF
Paris-G0N-HN-Gateway	ge-0/0/10.0 (8.8.8.1)	vpn	Zones trust	Exported Routes: Static, OSPF

- o. Click **Finish**.
7. If you have selected **Policy Based**:
  - a. The only **Type** option available is **Site To Site**.
  - b. Select the VPN profile from the **VPN Profile** menu.

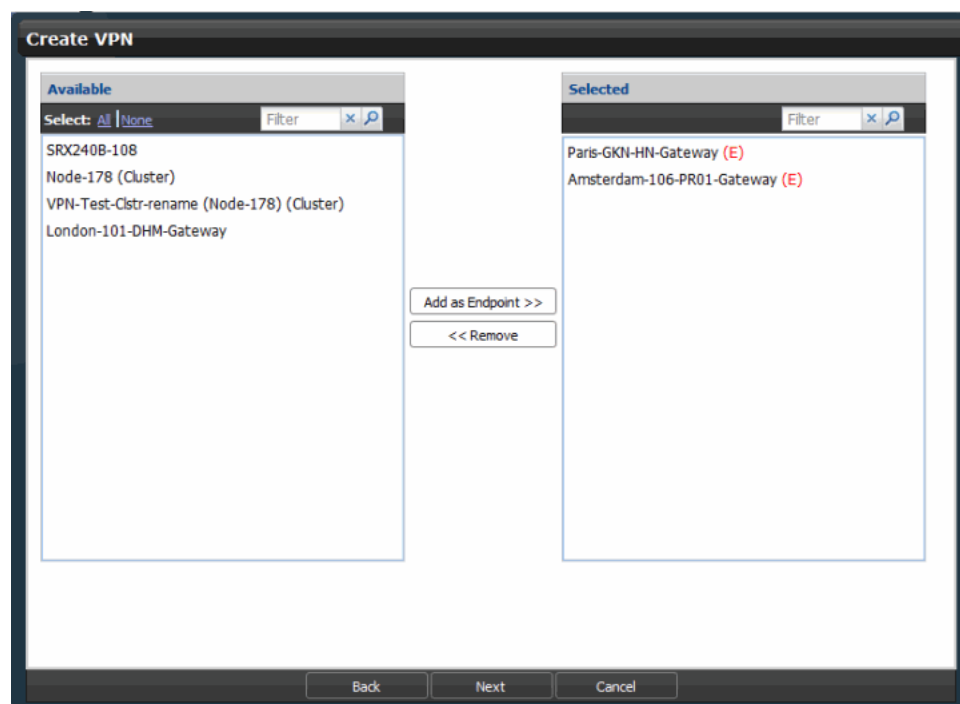


**NOTE:** If you choose to create a full-mesh VPN, you can choose only the Main mode profile as the VPN profile.

- c. Select the option button next to the type of preshared key you want to use.
  1. If you select **Autogenerate**, select the **Generate Unique key per tunnel** check box to generate a unique key per tunnel.
  2. If you select **Manual**, enter the manual key in the **Manual Key** field.
- d. Click **Next**.
 

The page displays the **Available** and **Selected** panes.
- e. Select the device from the **Available** column, and click **Add as Endpoint**, as shown in Figure 65 on page 139.

Figure 65: Create VPN Policy-Based—Add as Endpoint Page

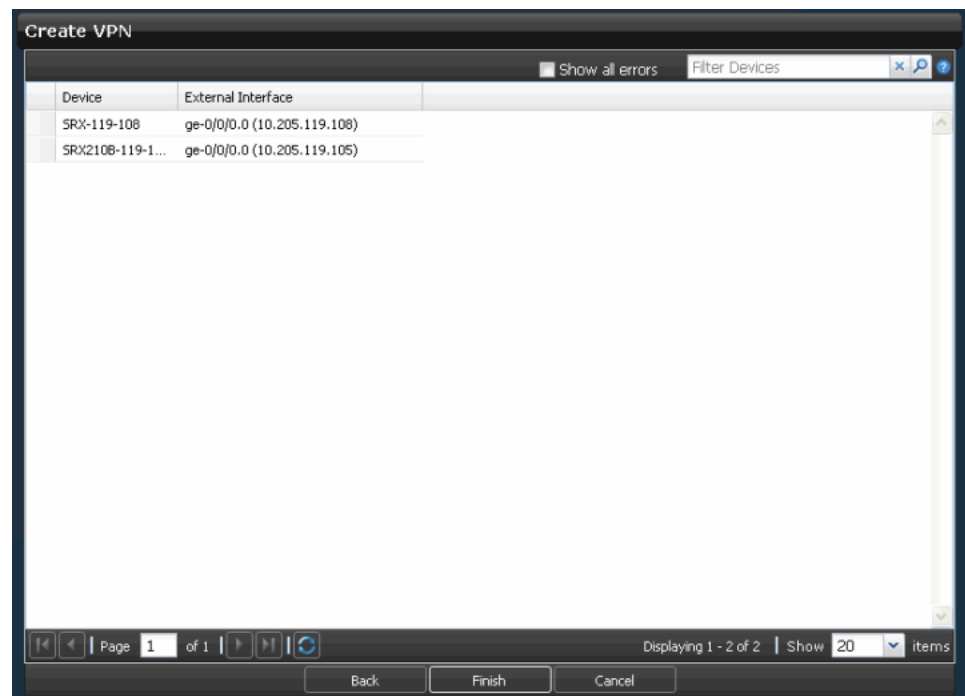


- f. Click **Next**.

The page that appears gives you a preview of the values you entered for the VPN, as shown in Figure. The page displays error indicators if the options you have configured do not map to the device. You can also click the **Show all Errors** check box to view all errors in the configuration. If errors are present, you must modify the configuration to eliminate them before you can proceed to the next step.

Select the external interface for the device from the list.

Figure 66: Create VPN Page—External Interface Selection



g. Click **Finish**.



**NOTE:** You cannot delete a policy-based VPN if the VPN is used in a firewall rule.



**NOTE:** Policy-based VPN is not supported on SRX Series logical systems. Security Design does not show logical systems when you select the policy-based VPN.



**NOTE:** In the dual hub scenario, if there are two paths available to reach a particular network, user has an option to set the metric value for each path and set the priority. Based on the metric value, user can select the appropriate path to reach the network. This is available only at the hub side and this option is available for both static and dynamic routing.



**NOTE:** When a default proposal definitions used (standard, compatible, and basic) in VPN profile for extranet devices, you might be able to find out what is required for an extranet device. You must use custom proposals if you select extranet device as an endpoint in VPN.



**NOTE:** When **Autogenerate** preshared key option is used for VPN design that involves the extranet device as endpoint, you can view SRX Series device tunnel endpoint settings, edit and unmask the key, and save the key as reference.

To perform an inline addition of the new VPN object:

1. Click the **Protected Zone/Networks** column for the available device. The VPN Policy Inline Object Creation page, as shown in [Figure 67 on page 141](#), appears. The page lists the zone or networks available for creating the VPN object.

**Figure 67: Inline Address Object Creation Page**

2. Click the plus sign (+) to create the new address object.
3. Click **Create** to create the object, or click **Cancel** to discard the changes.

## Publishing IPsec VPNs

To publish an IPsec VPN:

1. From the **Security Design** task ribbon, select **VPN > Publish VPN**.  
The **Services** page appears with all VPNs. It also displays the publish states of all the VPNs.
2. Select the check box next to the VPN that you want to publish.



**NOTE:** You can search for a specific device on which the VPN is published by entering the search criteria in the search field in the right top corner of the **Services** page. You can search the devices by their name, IP address, or the OS version.



**NOTE:** If the VPN is to be published on a large number of devices, the devices are displayed across multiple pages. You can use the pagination and display options available on the lower ribbon, just below the list of devices to view all devices on which the VPN is published.

3. Click the **Schedule at a later time** check box if you want to schedule and publish the configuration later.
4. Click **Next**.

The **Affected Devices** page displays the devices on which this VPN will be published.

5. If you want to preview the configuration changes that will be pushed to the device, click the **View** link in the **Configuration** column corresponding to the device. A **Configuration Preview** progress bar is shown while the configuration pushed to the device is generated.

The **CLI Configuration** tab appears by default. You can view the configuration details in the CLI format.

6. View the XML format of the configuration by clicking the **XML Configuration** tab.
7. Click **Back**.
8. Click **Publish** if you want to only publish the configuration.

A new job is created and the job ID appears in the **Job Information** dialog box.

9. Click **Publish and Update** if you want to publish and update the devices with the configuration.

The VPN is now moved into the Published state if the configuration is published to all devices involved in the VPN. If the configuration is not published to all devices involved in the VPN, the VPN is placed in the Partially Published state. If a VPN is created but not published, the VPN is placed in the Unpublished state. If any modifications are made to the VPN configuration after it is published, the VPN is placed in the Republish Required state. You can view the states of the VPN by hovering over them.

A new job is created and the job ID appears in the **Job Information** dialog box.

10. Click the job ID to view more information about the job created. This action directs you to the **Job Management** workspace.

If you get an error message during the publish or if the VPN publish fails, go to the Job Management workspace and view the relevant job ID to see why the publish failed.





**NOTE:** You can also publish a VPN by right-clicking the VPN in the VPN Tabular view and selecting **Publish VPN**. You are redirected to the **Affected Devices** page.

#### Related Documentation

- [IPsec VPN Overview on page 131](#)
- [Creating IPsec VPNs on page 132](#)
- [Managing IPsec VPNs on page 143](#)

## Managing IPsec VPNs

You can modify and delete the IPsec VPNs listed in the **Manage VPNs** page.

To open the **Manage VPNs** page:

- From the **Security Design** task ribbon, select **> VPN**.

The **Manage VPNs** page appears. All IPsec VPNs created so far are listed by default in the graphical view.

You can perform the following tasks in the **Manage VPNs** page:

1. [Modifying IPsec VPNs on page 143](#)
2. [Modifying Endpoint Settings in a VPN on page 144](#)
3. [Deleting IPsec VPNs on page 145](#)

## Modifying IPsec VPNs

To modify an IPsec VPN:

1. From the **Security Design** task ribbon, select **VPN**.

The VPN Tabular view appears.

2. Select the IPsec VPN that you want to modify from the left pane and click the appropriate link from the **Modify: General Settings : Device Association : Tunnel Settings** link on the right pane.

This action redirects you to the section of the IPsec VPN that you want to modify.



**NOTE:** You can modify all the parameters of the VPN except the type of VPN.

3. Click **Modify**.
4. Click **Save**.

To modify the global settings of the devices in a VPN:

1. From the **Security Design** task ribbon, select **VPN** .  
The VPN Tabular view appears.
2. Select the IPsec VPN that you want to modify from the left pane.  
This devices that are a part of the VPN are displayed in the right pane.
3. Click the **External Interface** field of the device whose external interface you want to modify and select the new external interface.
4. Click the **Tunnel Zone** field of the device whose tunnel zone you want to modify and select the new tunnel zone.
5. Click **OK**.
6. Click the **Protected Zone/Networks** field of the device that needs to be modified and select the new network or zone.
7. Click **OK**.
8. Click **Save**.
9. Click **OK**.

## Modifying Endpoint Settings in a VPN

To modify the endpoint settings in an IPsec VPN:

1. From the **Security Design** task ribbon, select **VPN** .  
The VPN Tabular view appears.
2. Select the device in the IPsec VPN that you want to modify from the left pane.  
The settings configured for the device are shown in the right pane. You can modify all settings of the device except the External Interface, Tunnel Interface, and Tunnel Zone settings.
3. For each endpoint device, you can modify the **VPN Name**, and **Preshared Key** fields, and customize the VPN. Click on the required endpoint device on the left pane, and you will get an option to change these fields on the right pane.
4. Click **Save**.

To modify the general settings of a VPN:

1. From the **Security Design** task ribbon, select **VPN** .  
The VPN Tabular view appears.
2. Select the IPsec VPN that you want to modify from the left pane.  
This devices that are a part of the VPN are displayed in the right pane.
3. Click the **General Settings** link at the top of the VPN Tabular view.

The **Modify General Settings** window appears. You can modify the name and description of the VPN, VPN profile, and the Preshared key fields.

4. Click **Modify**.



**NOTE:** You can also modify the device associations and tunnel settings of a VPN by clicking the **Device Associations** and **Tunnel/Route Settings** links, respectively on top of the VPN Tabular view.

## Deleting IPsec VPNs

To delete an IPsec VPN:

1. From the **Security Design** task ribbon, select **VPN**.  
The VPN Tabular view appears.
2. Right-click the IPsec VPN you intend to delete and click the **Delete VPN** link.  
A confirmation window appears.
3. Click **Delete**.



**NOTE:** If you delete a VPN, the erase configuration is sent to all devices that were a part of the VPN during the next **Update** operation for the device.

### Related Documentation

- [IPsec VPN Overview on page 131](#)
- [Creating IPsec VPNs on page 132](#)
- [Publishing IPsec VPNs on page 141](#)



## PART 6

# NAT Policies

- [NAT Policy on page 149](#)



## CHAPTER 17

# NAT Policy

- [NAT Overview on page 149](#)
- [Creating NAT Policies on page 151](#)
- [Adding Rules to a NAT Policy on page 156](#)
- [Ordering the Rules in a NAT Policy on page 160](#)
- [Publishing NAT Policies on page 161](#)
- [Managing NAT Policies on page 163](#)

## NAT Overview

---

Network Address Translation (NAT) is a form of network masquerading where you can hide devices between the zones or interfaces. A trust zone is a segment of the network where security measures are applied. It is usually assigned to the internal LAN. An untrust zone is the Internet. NAT modifies the IP addresses of the packets moving between the trust and untrust zones.

Whenever a packet arrives at the NAT device, the device performs a translation on the packet's IP address by rewriting it with an IP address that was specified for external use. After translation, the packet appears to have originated from the gateway rather than from the original device within the network. This helps you hide internal IP addresses from the other networks and keep your network secure.

Using NAT also allows you to use more internal IP addresses. Because these IP addresses are hidden, there is no risk of conflict with an IP address from a different network. This helps you conserve IP addresses.

Junos Space Security Design supports three types of NAT:

- **Source NAT**—Translates the source IP address of a packet leaving the trust zone (outbound traffic). It translates the traffic originating from the device in the trust zone. Using source NAT, an internal device can access the network by using the IP addresses specified in the NAT policy.
- **Destination NAT**—Translates the destination IP address of a packet entering the trust zone (inbound traffic). It translates the traffic originating from a device outside the trust zone. Using destination NAT, an external device can send packets to a hidden internal device.

- Static NAT—Always translates a private IP address to the same public IP address. It translates traffic from both sides of the network (both source and destination). For example, a Web server with a private IP address can access the Internet using a static, one-to-one address translation.

Junos Space Security Design provides you with a workflow where you can create and apply NAT policies on devices in a network.

Security Design views each logical system as any other security device and takes ownership of the security configuration of the logical system. In Security Design, each logical system is managed as a unique security device.



**NOTE:** If the root logical system is discovered, all other user logical systems inside the device, will be discovered by itself.

---

Because an SRX Series logical system device does not support interface NAT, Security Design also does not allow interface NAT configuration of logical system. The logical system cannot participate in group NAT in Security Design. For a device NAT policy, the interface based translation selection and pool with **Overflow Pool** as interface are not supported in logical systems. The configuration is validated during the publishing of the NAT policy to avoid commit failures in the device.

**Related  
Documentation**

- [Creating NAT Policies on page 151](#)
- [Publishing NAT Policies on page 161](#)
- [Managing NAT Policies on page 163](#)
- [Managing NAT Pools on page 53](#)



## Creating NAT Policies

To create a NAT policy:

1. From the **Security Design** task ribbon, select **NAT Policy**.

The NAT Policy Tabular view appears, as shown in [Figure 68 on page 151](#). NAT Policy Tabular view is a table with two panes. The left pane displays all the NAT policies in the system which includes device, group, and global NAT policies.

**Figure 68: NAT Policy Tabular View**

S.No.	Name	NAT Type	Original Packet Source Ingress Address	Original Packet Destination Egress Address Port	Translated Packet Source	Translated Packet Destination	Description
1	Corp-gateSOURCE	Static	Zones: CL-DMZ-SVR5-INNE, ECM-DMZ-SVR5-INNE	Zones: China-V4-Network, CL-DMZ-SVR5-OUT, ECM-DMZ-SVR5-OUT	Any	Any	Interface
2	Corp-gateSOURCE	Dynamic	Zones: CL-DMZ-VDC	Zones: China-V4-Network, DMZ	Corp-DMZ-2, Corp-DMZ-1	Any	Pool Pool Name: PublicChina
3	Corp-gateSTATIC	Static	Zones: DMZ, DMZ-VDC	Not Applicable	Not Applicable	ge1-11	Not Applicable
4	Corp-gateDESTINATION	Destination	Zones: CL-DMZ-VDC, ECM-DMZ-SVR5-INNE	ALL-WEB_GROUP	Not Applicable	WEB-Rak-2	Any
5	Corp-gateDESTINATION	Destination	Zones: DMZ, DMZ-VDC	India-Network	Not Applicable	WebServer1	8080

You can search for NAT policies in the left pane using NAT policy names and devices used in the NAT policy. You can search the rules in the right pane using NAT rule type, original packet source, original packet destination, translated packet source, translated packet destination, and the description used in the rule.

Tooltip view is available to show the object value information for the objects that you are using within the policies. Mouse over the source address or destination address and objects information is provided in the tool tip, as shown in figure. The tooltip contains address group name, value of the address such as IP, and subnet.

2. Click **Create NAT Policy** from the task ribbon.

The **Create NAT Policy** page appears. You can create a group policy or a device policy on this page.

3. To create a group policy:
  - a. Enter the name of the group policy in the **Name** field.
  - b. Enter a description for the group policy rules in the **Description** field. Security Design sends the comments entered in this field to the device.
  - c. Click the **Show Assigned Devices** check box to make devices on which policies have been configured available for selection.

- d. Select the devices on which the group policy will be published in the **Select Devices** pane. Select the devices from the **Available** column and click the right arrow to move these devices to the **Selected** column.

You can also search for the devices by entering the device name, device IP address, or device tag in the **Search** field in the **Select Devices** section. Once the searched devices are displayed, you can move them to the **Selected** column as shown in [Figure 69 on page 152](#).

Figure 69: Create NAT Policy Page

The screenshot shows the 'Create NAT Policy' window. At the top, 'Type' is set to 'Group' (radio button selected). Below it, 'Name' is 'Bng\_Lab' and 'Description' is an empty text box. A 'Show Assigned Devices' checkbox is present but unchecked. The 'Select Devices' section has a search filter and two columns: 'Available' and 'Selected'. The 'Available' column lists IP addresses from 10.205.230.10 to 10.205.230.7. The 'Selected' column lists 10.205.230.1 and 10.205.230.3. Arrows between the columns allow moving devices. At the bottom are 'Create' and 'Cancel' buttons.

- e. Click **Create**.



**NOTE:** One device can hold configuration data related to one NAT policy only. Therefore you cannot share devices for multiple NAT policies.

4. To create a device policy:
  - a. Enter the name of the device policy in the **Name** field.
  - b. Enter a description for the device policy in the **Description** field.
  - c. Select the device on which the device policy will be published from the **Device** menu.
  - d. Click **Create**.

To perform an inline addition of a new NAT pool object in the source NAT pool:

1. Click on the **Translated Packet Source** and select the **Translation Type** as Pool.

Figure 70: Setting Source NAT Pool Page

2. Click the plus sign to create the source NAT pool.

Figure 71: Create Source NAT Pool Page

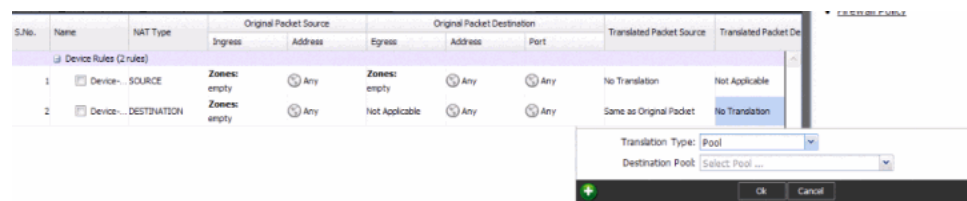
You can select **No Translation**, **Port/Range**, or **Overload** for the **Translation** field.

3. Click **Create** to create the source NAT pool or **Cancel** to discard the changes.

To perform inline addition of a new NAT pool object in the destination NAT pool:

1. Click on **Translated Packet Destination** and select **Pool** for the **Translation Type**.

Figure 72: Setting the Destination Pool Page



2. Click the plus sign (+) to create the destination NAT pool.

Figure 73: Create Destination NAT Pool Page

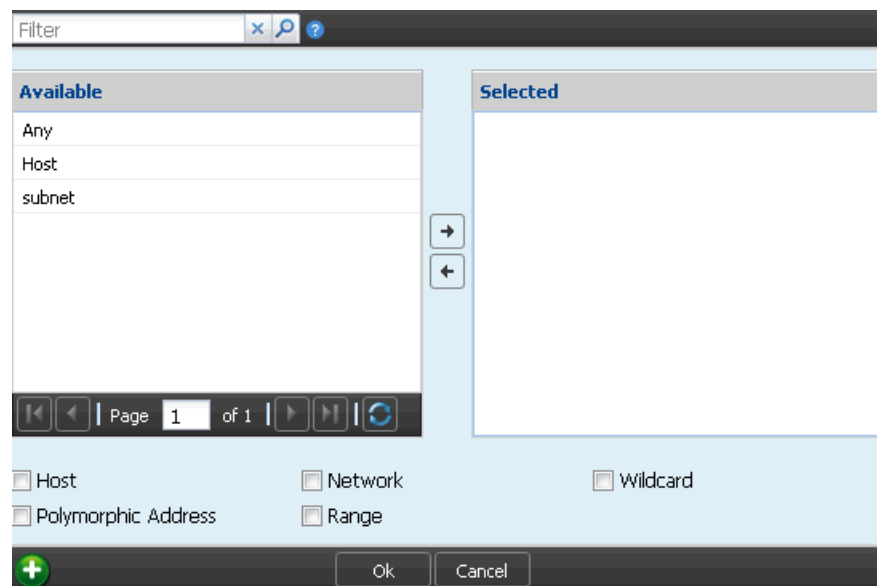
The dialog box has fields for 'Name:', 'Description:', 'Pool Address: Select Address', and 'Port:'. At the bottom are 'Create' and 'Cancel' buttons.

3. Click **Create** to create the destination NAT pool or **Cancel** to discard the changes.

To create address objects for the NAT policy:

1. Click on the source address. The following window appears with the available addresses to create the objects:

Figure 74: Create Inline NAT Address Object



2. Click on the plus sign (+) to create the new address object for NAT policy.

Figure 75: Create NAT Address Page

**Create Address**

Name:

Description:

Type: Host

IP    Host Name

3. Click **Create** to create the new address object or **Cancel** to discard all changes.



**NOTE:** Advanced NAT pool options must be modified from the Object Builder workspace in the NAT pool ILP.

**Related  
Documentation**

- [Adding Rules to a NAT Policy on page 156](#)
- [Ordering the Rules in a NAT Policy on page 160](#)
- [Publishing NAT Policies on page 161](#)
- [Managing NAT Policies on page 163](#)

## Adding Rules to a NAT Policy

---

When a new NAT policy is created, by default the policy displays links to create rules for the policy. If you have created a group NAT policy, you will see a **Create Source Rule** link in the right hand pane. If you have created a device NAT policy, you will see **Create Source Rule**, **Create Destination Rule**, and **Create Static Rule** links.

Depending on the type of rule you have chosen, some fields in the rule will not be applicable. If you choose a Source NAT rule, the **Translated Packet Destination** field will not be applicable. If you choose a Destination NAT rule, the **Egress** field in the **Original Packet Destination** column and the **Translated Packet Source** fields are not applicable. If you choose a Static NAT rule, the **Address** field in the **Original Packet Source** column, **Egress** field in the **Original Packet Destination** column, **Port** field in the **Original Packet Destination** column, and the **Translated Packet Source** fields are not applicable.

In addition to defining rules between zones and interfaces, the NAT rules can be defined with virtual routers defined on the device. These rules can be successfully published and updated on the device.

The Proxy ARP option is available under different fields based on the type of rule you have chosen. With a Static NAT rule, the Proxy ARP option is available under the **Translated Packet Source** field. With the Destination NAT rule and Static NAT rule, the Proxy ARP option is available under the **Address** field in the **Original Packet Destination** column.

The Proxy ARP feature also automatically selects the interface based on the **Egress** field for Source NAT rule and the **Ingress** field for Destination NAT rule and Static NAT rule.

To add rules to a NAT policy:

1. From the **Security Design** task ribbon, select **NAT Policy**.

The NAT Policy Tabular view appears.

2. Click the NAT policy you want to add rules to from the left pane.

The existing rules of the NAT policy are displayed in the right pane.

3. Click the **Add Rule** icon and select the type of rule you want to add.

A new rule is added in the bottom-most row depending on the type of rule you have added. The rule is assigned a serial number based on the number of rules already added to the policy. By default, the zones are set to Empty and the address and port of the packet source and packet destination are set to Any. The Translated Source and Translated Packet Source columns are either set to No Translation or Not Applicable, depending on the rule you are adding.

4. Click the **Name** field in the rule and change the name of the rule.

5. Click the **Ingress** field in the **Original Packet Source** column and select the appropriate zone or interface or routing instance.

The Zone or Interface or routing instance selector appears.

6. Select the appropriate option from the **Source Traffic Matching Type** drop-down menu.
7. In the zone or interface or routing instance selector, select the zones or interfaces or routing instance you want to associate the rule to, from the **Available** column.

On selection of **Routing Instance** option, you can select one or more of the available virtual routers on the device. For the group NAT policy, the consolidated list of all virtual routers on all devices that the policy is assigned to will be listed.

8. Click the right arrow in the selector.

The selected zones or interfaces or virtual routers are now moved to the **Selected** column.

9. Click **OK**.

10. Click the **Address** field in the **Original Packet Source** column and select the appropriate addresses.

The Address selector appears.

11. In the address selector, select the addresses you want to associate the rule to, from the **Available** section.

12. Click the right arrow in the selector.

The selected addresses are now moved to the **Selected** section.

13. Click **OK**.

14. Click the **Egress** field in the **Original Packet Destination** column and select the appropriate zone or interface or routing instance.

The zone or interface or routing instance selector appears.

**Figure 76: Destination Traffic Match Type Selector Page**

Destination Traffic Matching Type: Interface

**Available**

- Interface
- Zone
- Routing Instance

→

←

Ok Cancel

15. Select the appropriate option from the **Destination Traffic Matching Type** list.
16. In the zone or interface or routing instance selector, select the zones and interfaces or routing instance you want to associate the rule to, from the **Available** column.
17. Click the right arrow in the selector.

The selected zones or interfaces or routing instance are now moved to the **Selected** column.

The following [Figure 77 on page 158](#) shows the routing instance selection for the device:

**Figure 77: Routing Instance Selection Page**

18. Click **OK**.

19. Click the **Address** field in the **Original Packet Destination** column and select the appropriate addresses.

The Address selector appears.

20. In the address selector, select the addresses you want to associate the rule to, from the **Available** column.

21. Click the right arrow in the selector.

The selected addresses are now moved to the **Selected** column.

22. Click **OK**.

23. Click the **Port** field in the **Original Packet Source** column.

The Port selector appears.

24. Select the appropriate port type from the **Port Type** drop-down menu.

25. Click **OK**.

26. Click the **Translated Packet Source** field.

27. Select the appropriate translation type from the **Translation Type** drop-down menu.

- a. If you select **Pool** as the option from the **Translation Type** drop-down, you will see that there will be new fields to specify.
- b. Select the appropriate NAT pool from the **Source Pool** drop-down menu.  
All relevant options from the NAT pool you have chosen are displayed.
- c. Select the **Configure Proxy ARP** check box to enable the proxy ARP feature.
- d. Select the check boxes next to the address ranges you want to include and select the appropriate interface.



28. Click **OK**.

29. Click the **Destination Address** field in the **Translated Packet Destination** column and select the appropriate addresses.

This option is available only for destination NAT rule.



**NOTE:** For static NAT rule, you can configure **Routing Instance** from the **Translated Packet Destination** column.

30. Select the type of translation from the **Translation Type** drop-down menu.

31. Select the appropriate NAT pool from the **Destination Pool** drop-down menu.



**NOTE:** If you are creating a static NAT rule, the **Translated Address** list appears. You can select the appropriate address from the list.

32. Click **OK**.

33. Click the **Port** field in the **Translated Packet Destination** column.

The Port selector appears.

34. Select the appropriate port type from the **Port Type** drop-down menu.

35. Click **OK**.

36. Click the **Description** field and enter a description for the rule.

37. Click **Save**.

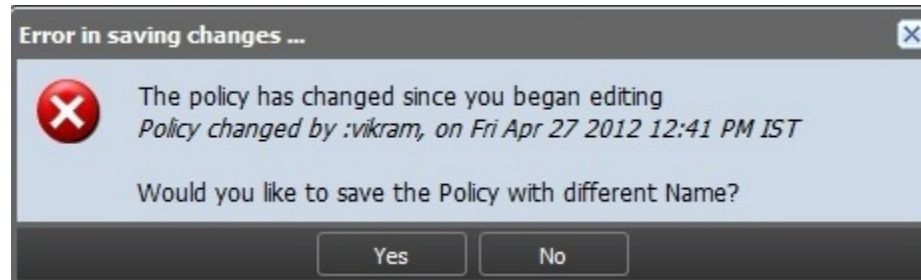


**NOTE:** You should click **Save** to save any changes you have made to the NAT policy. While in the process of making changes to the NAT policy, If you click on any of the tasks in the task ribbon before saving the NAT policy changes, all changes you have made will be lost. If you click anywhere inside the NAT Policy Tabular view, you will see a confirmation window to save the changes you have made.



**NOTE:** If another user has added new rules to the same policy, modifies the existing rules, or delete existing rules, and the user has already saved the changes before you, the following error message is received.

Figure 78: Concurrent NAT Policy Editing Error



The error message provides the user name and time at which changes are made to the policy. Whoever saves the changes first gets the preference to save the new rules added. You will be given an option to save your policy changes with different name. Click on Yes to save the policy with different name. Only saved rules are published to the policy.

#### Related Documentation

- [Ordering the Rules in a NAT Policy on page 160](#)
- [Publishing NAT Policies on page 161](#)
- [Managing NAT Policies on page 163](#)

## Ordering the Rules in a NAT Policy

To reorder the rules in a NAT policy:

1. From the **Security Design** task ribbon, select **NAT Policy**.  
The NAT Policy Tabular view appears.
2. Select the NAT policy whose rules you want to reorder.  
The rules of the NAT policy are displayed in the right pane.
3. Select a rule that you want to reorder and click the appropriate icon on the top of the right pane.

Icon Name	Description
Move Rule Up	Moves the rule one level up in the hierarchy.
Move Rule Down	Moves the rule one level down in the hierarchy.
Move Rule to Top	Moves the rule to the top of the hierarchy.
Move Rule to Bottom	Moves the rule to the bottom of the hierarchy.

The rule is now positioned accordingly. When the NAT policy is provisioned, the rules are provisioned to the devices in the order you have specified.

- Related Documentation**
- [Creating NAT Policies on page 151](#)
  - [Adding Rules to a NAT Policy on page 156](#)
  - [Publishing NAT Policies on page 161](#)
  - [Managing NAT Policies on page 163](#)

## Publishing NAT Policies

To publish a NAT policy:

1. From the **Security Design** task ribbon, select **NAT Policy** > **Publish policy**.

The **Services** page appears with all the NAT policies. It also displays the publish states of the NAT policies.

2. Select the check box next to the NAT policy that you want to publish.



**NOTE:** You can search for a specific device on which the policy is published by entering the search criteria in the Search field, on the right top corner of the **Services** page. You can search the devices by their name, IP address, and device tags.



**NOTE:** If the NAT policy is to be published on a large number of devices, the devices are displayed across multiple pages. You can use the pagination and display options available on the lower ribbon, just below the list of devices to view all devices on which the policy is published.

3. Select the **Schedule at a later time** check box if you want to schedule and publish the configuration later.
4. Click **Next**.

The **Affected Devices** page displays the devices on which this NAT policy will be published.

5. If you want to preview the configuration changes that will be pushed to the device, click the **View** link in the **Configuration** column corresponding to the device. A **Configuration Preview** progress bar is shown while the configuration pushed to the device is generated.

The **CLI Configuration** tab appears by default. You can view the configuration details in CLI format.

Figure 79: NAT Policy CLI Configuration

```

##source-nat-rule-set##
set security nat source rule-set 34022
set security nat source rule-set 34022 from interface ge-0/0/1.0
set security nat source rule-set 34022 from interface ge-0/0/2.0
set security nat source rule-set 34022 to routing-instance OFF
set security nat source rule-set 34022 rule Device-1 match source-address 0.0.0.0/0
set security nat source rule-set 34022 rule Device-1 match destination-address 1.1.1.1
set security nat source rule-set 34022 rule Device-1 then source-nat pool pool1
##pool##
set security nat source pool pool1 address 12.1.1.0/24
set security nat source pool pool1 port no-translation
##proxy-arp##
set security nat proxy-arp interface ge-0/0/3.1900 address 12.1.1.1 to 12.1.1.254

```

6. View the XML format of the configuration by clicking the **XML Configuration** tab.
7. Click **Back**.
8. Click **Publish** if you want to only publish the configuration.

A new job is created and the job ID appears in the **Job Information** dialog box.

9. Click **Publish and Update** if you want to publish and update the devices with the configuration.

The NAT policy is now moved into the Published state if the configuration is published to all devices involved in the policy. If the configuration is not published to all devices involved in the NAT policy, the NAT policy is placed in the Partially Published state. If a NAT policy is created but not published, the NAT policy is placed in the Unpublished state. If any modifications are made to NAT policy configuration after it is published, the NAT policy is placed in the Republish Required state. You can view the states of the NAT policy by hovering over them.

A new job is created and the job ID appears in the **Job Information** dialog box.

10. Click the job ID to view more information about the job created. This action directs you to the **Job Management** workspace.

If you get an error message during the publish or if the NAT policy publish fails, go to the Job Management workspace and view the relevant job ID to see why the publish failed.



**NOTE:** You can also publish a NAT policy by right-clicking the NAT policy in the NAT Policy Tabular view and selecting **Publish NAT Policy**. You are redirected to the **Affected Devices** page.

- Related Documentation**
- [Creating NAT Policies on page 151](#)
  - [Adding Rules to a NAT Policy on page 156](#)
  - [Ordering the Rules in a NAT Policy on page 160](#)
  - [Managing NAT Policies on page 163](#)

## Managing NAT Policies

---

- [Modifying NAT Policies on page 163](#)
- [Deleting NAT Policies on page 163](#)
- [Cloning NAT Policies on page 164](#)
- [Exporting a NAT Policy on page 164](#)
- [Deleting Rules in a NAT Policy on page 164](#)
- [Grouping Rules in a NAT Policy on page 165](#)
- [Enabling/Disabling Rules in a NAT Policy on page 165](#)
- [Copying and Pasting Rules in a NAT Policy on page 166](#)
- [Assigning Devices to a NAT Policy on page 167](#)
- [Deleting Devices from a NAT Policy on page 167](#)

### Modifying NAT Policies

To modify a NAT policy:

1. From the **Security Design** task ribbon, select **NAT Policy**.  
The NAT Policy Tabular view appears.
2. Right-click the NAT policy you want to modify from the left pane and select **Modify Policy**.  
The **Edit Policy** window appears. You can modify the name and description of the NAT policy.
3. Click **Modify**.

### Deleting NAT Policies

To delete a NAT policy:

1. From the **Security Design** task ribbon, select **NAT Policy**.  
The NAT Policy Tabular view appears.
2. Right-click the NAT policy you want to delete and select **Delete Policy**.  
A confirmation window appears.
3. Click **Yes**.



**NOTE:** If you delete a NAT policy, the erase configuration is sent to all devices that were a part of the NAT policy during the next **Update** operation for the device.

## Cloning NAT Policies

To clone a NAT policy:

1. From the **Security Design** task ribbon, select **NAT Policy**.  
The NAT Policy Tabular view appears.
2. Right-click the NAT policy you want to clone and select **Clone Policy**.  
The **Clone Policy** window appears. You can modify the name and description mode of the NAT policy.
3. Click **Clone**.

## Exporting a NAT Policy

To export a NAT policy:

1. From the **Security Design** task ribbon, select **NAT Policy**.  
The NAT Policy Tabular view appears.
2. Right-click the NAT policy you want to export and select **Export Policy**.  
The **Export Policy** window appears.
3. Click **Export**.

## Deleting Rules in a NAT Policy

To delete rules in a NAT policy:

1. From the **Security Design** task ribbon, select **NAT Policy**.  
The NAT Policy Tabular view appears.
2. Select the NAT policy whose rules you want to delete.  
The rules of the NAT policy appears in the right pane.
3. Select the check boxes next to the rules that you want to delete.
4. Click the **Delete Rule** icon on the top of the right pane.

## Grouping Rules in a NAT Policy

To group rules in a NAT policy:

1. From the **Security Design** task ribbon, select **NAT Policy**.  
The NAT Policy Tabular view appears.
2. Select the NAT policy whose rules you want to group.  
The rules of the NAT policy are displayed in the right pane.
3. Select the check boxes next to the rules you want to group.
4. Right-click the rules and select **Rule Group > Create Rule Group**.  
The **Create Rule Group** window appears.
5. Enter a name for the rule group in the **Name** field.
6. Enter a description for the rule group in the **Description** field.
7. Click **Create**.



**NOTE:** When the rule group is created, you can add a rule into the rule group, modify the rule group name, move the rule into another rule group, ungroup rules, and ungroup rule groups using appropriate options.

## Enabling/Disabling Rules in a NAT Policy

To enable or disable rules in a NAT policy:

1. From the **Security Design** task ribbon, select **NAT Policy**.  
The NAT Policy Tabular view appears.
2. Select the NAT policy whose rules you want to enable or disable.  
The rules of the NAT policy appears in the right pane.
3. Select the check boxes next to the rules that you want to enable or disable.
4. Click the **Enable** or **Disable** icon.



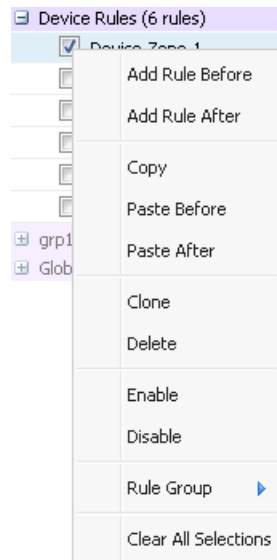
**NOTE:** You can enable or disable a rule group. When a rule group is disabled, all rules in the rule group are also disabled. The rule group row in the Tabular view is greyed out but the rules are not greyed out. However, the rules in the rule group are not published to the device during the publish operation, if they are disabled.

## Copying and Pasting Rules in a NAT Policy

To copy and paste rules in a NAT policy:

1. On the right pane, select the device rule that must be copied. Right-click on the selected device rule, and select **Copy**.

**Figure 80: Rule Copy Paste Options**

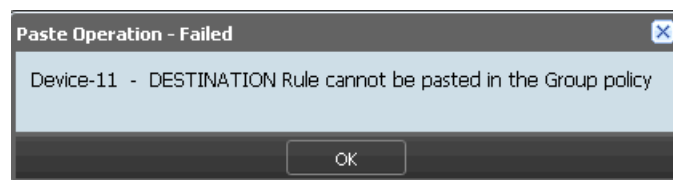


2. On the left pane, select the NAT policy that you want to paste the rule. On the right pane, right-click on the device rule that you want the rule to be pasted. You can paste the rule before the selected device rule or after the selected device rule by choosing the options **Paste Before** or **Paste After**.

Rule paste fails under the following conditions:

- If you copy the Destination NAT rule and paste the rule in the group policy, error shown in [Figure 81 on page 166](#) appears.

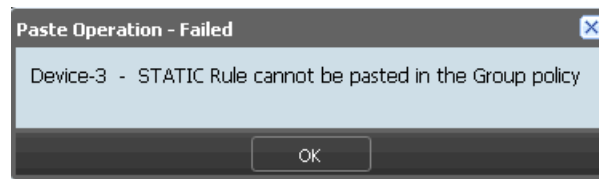
**Figure 81: Destination NAT Rule Paste Error**



- If you copy the Static NAT rule and paste the rule in the group policy, error shown in [Figure 82 on page 167](#) appears.

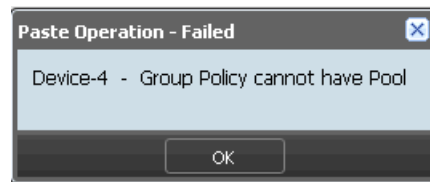


Figure 82: Static NAT Rule Paste Error



- If you copy a source rule of translation type Pool to the group rule, error shown in [Figure 83 on page 167](#) appears.

Figure 83: Group Policy Paste Error



## Assigning Devices to a NAT Policy

To assign devices to a group NAT policy:

1. From the **Security Design** task ribbon, select **Firewall Policy**.  
The Policy Tabular view appears.
2. Right-click the NAT policy to which you want to assign devices and select **Assign Devices**.  
The **Assign Devices to Service** window appears.
3. Select the devices that need to be added to the NAT policy in the **Select Devices** pane. Select the devices from the **Available** column and click the right arrow to move these devices to the **Selected** column.
4. Click **Modify**.

## Deleting Devices from a NAT Policy

To delete devices from a group NAT policy:

1. From the **Security Design** task ribbon, select **Firewall Policy**.  
The Policy Tabular view appears.
2. Right-click the NAT policy from which you want to delete devices and select **Assign Devices**.  
The **Assign Devices to Service** window appears.
3. Select the devices that need to be deleted from the NAT policy in the **Select Devices** pane. Select the devices from the **Selected** column and click the left arrow to move these devices to the **Available** column.
4. Click **Modify**.



.....

**NOTE:** Deleting a device from a group NAT policy creates a device NAT policy. This policy carries all the device-exception rules of the device from the group NAT policy.

.....

**Related  
Documentation**

- [Creating NAT Policies on page 151](#)
- [Adding Rules to a NAT Policy on page 156](#)
- [Ordering the Rules in a NAT Policy on page 160](#)
- [Publishing NAT Policies on page 161](#)

## PART 7

# Global Search

- [Global Search on page 171](#)



# Global Search

- [Global Search on page 171](#)

## Global Search

The Security Design home page provides a global search option to find objects and security configurations. You can also click on a search result and navigate to its page.

To search for objects or configurations using the Global search:

1. Enter the search criteria in the **Search** field and click the magnifying glass icon.

All objects and configurations matching the search criteria appear in the search results page. The area on the left displays the search results with appropriate filters and the area on the right displays the detailed search results with a short description as shown in [Figure 84 on page 171](#).

Figure 84: Global Search Results



2. Click a detailed search result URL to navigate to its respective page.

The search results for Global search are based on how the Security Design objects and configurations are indexed. [Table 10 on page 171](#) specifies the objects and configurations that you can search using Global search.

Table 10: Security Design Global Search

Security Design Object/Configuration	Attributes by which Global Search is possible.
--------------------------------------	--

Table 10: Security Design Global Search (*continued*)

Firewall Policy	Name, profile name, description, source address , destination address, service, and zone.
Address	Addresses that are IP, subnet, range, and hostname type.
Address Group	All address part of the group after expanding address groups within the group
Service	Services that include ports, ICMP, RPC, and UUID searches.
Service Group	All service part of the group.
VPN	All addresses used in VPN or protected resources of the VPN.
NAT	All address used in NAT, NAT pools, and Match Type (zone, interface).

You cannot search objects such as device name, policy profile, and template using Global search. If you type a valid IPv4 address, subnet or range search results return all addresses that include that specific valid IPv4 address. For example, if you type 1.1.1.1 and if there is an subnet address 1.1.1.0/24, the search result will match the subnet and return the result.

With Global search, the search is free-text based. You can search for phrases and multiple terms. The default value for multiple terms is the OR operator. You can also search for multiple terms using the AND operator. By default, the search query looks at name, IP, port, category, ICMP code, ICMP type, subnets, and IP ranges. All search results are highlighted as part of the result and the search results have a URL to jump to the corresponding object in its ILP. The IP address searches looks for an ip within ranges and subnets as long as User gives a valid IP address. 6) Range based searches for IP addresses; you would need to add the – for range. For example, 1.1.1.1/24, and 10.204.76.56-10.204.76.80. The subnet searches should be provided with valid subnets. All port specific searches will search for ports only. The source port uses the keyword “srcPort” and the destination port uses keyword “dstPort”.

SD Search supports wildcard searches if user uses “\*” character in the search query. Names of objects will be broken down into one or more terms if the name has a non letter character or a number. For example, a name like “enet\_dest12” will be broken into “enet” “dest” and “12”. Youd can search on “enet” “dest” or 112 or type “ene\*” “des\*” etc.

## PART 8

# Downloads

- [Downloads on page 175](#)





## CHAPTER 19

# Downloads

- Downloading the Signature Database on page 175
- Installing the Signature Database on page 177

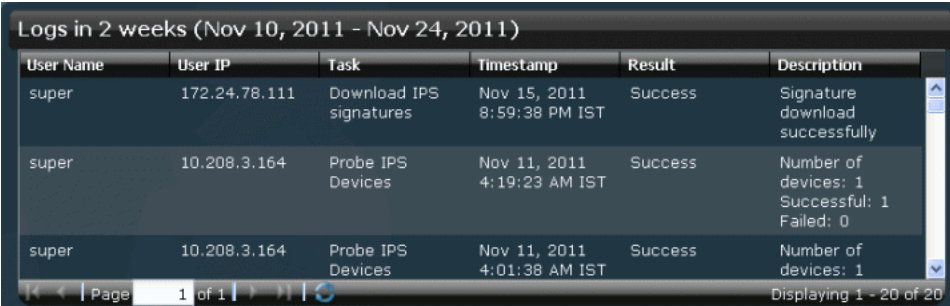
### Downloading the Signature Database

To download the Signature database:

1. From the **Security Design** task ribbon, select **Download**.

You can see the last log date in the last two weeks as shown in [Figure 85 on page 175](#).

**Figure 85: Signature Download Logs**



User Name	User IP	Task	Timestamp	Result	Description
super	172.24.78.111	Download IPS signatures	Nov 15, 2011 8:59:38 PM IST	Success	Signature download successfully
super	10.208.3.164	Probe IPS Devices	Nov 11, 2011 4:19:23 AM IST	Success	Number of devices: 1 Successful: 1 Failed: 0
super	10.208.3.164	Probe IPS Devices	Nov 11, 2011 4:01:38 AM IST	Success	Number of devices: 1

Page 1 of 1 | Displaying 1 - 20 of 20

2. Select **Signature Database** from the **Downloads** workspace.

The **Signature Database** page appears, as shown in [Figure 86 on page 176](#). You can see the active databases that were downloaded earlier.

Figure 86: Signature Database Page

**Signature Database**

Active Database on Space

Database Version	Publish date	Update Job	Installed Device Count	Detectors	Action
2030	2011-11-15 12:16:19	327686	0	5.1.110110809...	Install

**Latest list for IPS signatures**

Search Version:

Database Version	Publish date	Update Summary	Detectors	Action
2035 (latest)	2011-11-23 12:16:06	1 new signatures 2 updated signatures	11.6.140110920...	Download
2034	2011-11-22 12:02:12	6 new signatures 6 updated applications	11.6.140110920...	Download
2033	2011-11-21 12:04:41	19 new signatures 4 updated signatures	11.6.140110920...	Download
2032	2011-11-17 13:00:49	1 new signatures 2 updated signatures 22 updated applications	11.6.140110920...	Download
2031	2011-11-16 14:02:29	10 new signatures 2 updated signatures 2 renamed signatures	11.6.140110920...	Download
2029	2011-11-14 11:59:16	7 new signatures 4 new applications 5 updated signatures 1 renamed signatures	11.6.140110920...	Download

3. Select **Download Configuration**.

The **Download Configuration** page appears, as shown in Figure 87 on page 176.

Figure 87: Download Configuration Page

**Download Configuration**

Download URL:

**Use Proxy Server**

Enable Proxy: ☐

Host Name:

Host Port:

User Name:

User Password:

☒ **Schedule at a later time**

Date and time:

☒ **Repeat**

☐ **End Time**

4. Enter the URL from where you want to download the AppSecure database in the **Download URL** field.
5. Click the **Enable Proxy** check box.
6. Enter the hostname in the **Proxy Host Name** field.
7. Enter the host's port number in the **Proxy Host Port** field.

8. Enter the username in the **Proxy User Name** field.
9. Enter the password in the **Proxy User Password** field.
10. Select the **Schedule at a later time** check box or down arrow to view the scheduling options.
11. Enter a date in the **Date and time** field. You can also choose a date from the date picker by clicking the date picker icon.
12. Select the time from the drop-down menu.
13. Select the **Repeat** check box to enable the schedule to recur in a given time interval.
14. Enter a numerical value in the first field in this section.
15. Select the appropriate length of time from the drop-down menu below the first field.
16. Select the **End Time** check box to view the options available to set the end time for recurring downloads.
17. Enter a date in the **Date and time** field. You can also choose a date from the date picker by clicking the date picker icon.
18. Select the time from the drop-down menu.
19. Click **Download**.

**Related Documentation** • [Installing the Signature Database on page 177](#)

---

## Installing the Signature Database

To install the signature database:

1. From the **Security Design** task ribbon, select **Downloads**.  
You can see the last login date in the last two weeks.
2. Select **Signature Database** from the **Downloads** workspace.

The **Signature Database** page appears. You can see the active database that was downloaded earlier.

3. Select **Install Configuration**.

The **Install Configuration** page appears, as shown in [Figure 88 on page 178](#).

Figure 88: Install Configuration Page

**Install Configuration**

☒ **Signature Summary**

Device name	Device IP	Platform	OS Version	Attack Version	Detector Version	Connection Status
fib	10.208.130.213	SRX650	11.4R1.2	2035	11.6.160110920	up

Page 1 of 1 | Probe IPS Devices | Displaying 1 - 1 of 1 | Show 25 items

☒ **Schedule at a later time**

Date and time: 11/24/11 7:52 AM IST

☒ **Repeat**

1  
Hours

☒ **End Time**

Date and Time: 11/24/11 7:53 AM IST

**Install** **Cancel**

4. Click the down arrow next to **Signature Summary** to view the version of the database and platforms that support this database.
5. Click the check box next to the devices on which you want to install the database.
6. Select the **Schedule at a later time** check box or click the down arrow to view the scheduling options.
7. Enter a date in the **Date and time** field. You can also choose a date from the date picker by clicking the date picker icon.
8. Select the time from the drop-down menu.
9. Click the downward pointing arrow next to the **Repeat** section to enable the schedule to recur in a given time interval. You can also click the check box next to **Repeat** section to enable the schedule to recur in a given time interval.
10. Enter a numerical value in the first field in this pane.
11. Select the appropriate length of time from the drop-down menu below the first field.
12. Click the downward pointing arrow next to the **End Time** section to view the options available to set the end time for recurring installations. You can also click the check box next to **End Time** section to view the options available to set the end time for recurring installations.
13. Enter a date in the **Date and time** field. You can also choose a date from the date picker by clicking the date picker icon.
14. Select the time from the drop-down menu.
15. Click **Install**.



NOTE: Only 'primary' SRX node is discovered by Security Design. If a job is created to install IPS signature on the primary SRX node, the IPS signature is automatically installed on the SRX secondary node also.

**Related  
Documentation**

- [Downloading the Signature Database on page 175](#)



## PART 9

# IPS Management

- [IPS Management Overview on page 183](#)
- [IPS Management on page 185](#)





## CHAPTER 20

# IPS Management Overview

- [IPS Management Overview on page 183](#)

## IPS Management Overview

---

You can use the IPS Management workspace to download and install the AppSecure signature database to security devices. You can automate the download and install process by scheduling the download and install tasks and configure these tasks to recur at specific time intervals. This ensures that your signature database is up-to-date.

You can view the predefined IPS policy templates and create customized IPS policy-sets in this workspace. You can also enable IPS configuration in a firewall policy and provision IPS related configuration with firewall policy.

### Related Documentation

- [Downloading the Signature Database on page 175](#)
- [Installing the Signature Database on page 177](#)



## CHAPTER 21

# IPS Management

- [Creating IPS Signatures on page 185](#)
- [Managing IPS Signatures on page 187](#)
- [Creating IPS Signature Sets on page 191](#)
- [Adding Rules to an IPS Signature Set on page 192](#)
- [Managing IPS Signature Sets on page 193](#)
- [Creating IPS Policies on page 195](#)
- [Publishing IPS Policies on page 198](#)
- [Managing IPS Policies on page 201](#)

### Creating IPS Signatures

---

To create an IPS signature:

1. From the **Security Design** task ribbon, select **IPS Management**.  
The **IPS Policies** page appears with all IPS policies.
2. Click **IPS Signature**.

All IPS signatures that are downloaded appears in the **View All IPS Signatures** page, as shown in [Figure 89 on page 186](#). This page displays the version of the signature database. The left pane displays the different categories of signature and the right pane displays the signatures.

Figure 89: View All IPS Signatures Page

Name	Severity	Category	Object Type	Recommended	Pre-defined/Custom
Additional Web Services - Critical	Critical	SSL,FTP,WORM,GOPHER	Dynamic Group	No	Pre-defined
Additional Web Services - Info	Info	SSL,FTP,WORM,GOPHER	Dynamic Group	No	Pre-defined
Additional Web Services - Major	Major	SSL,FTP,WORM,GOPHER	Dynamic Group	No	Pre-defined
Additional Web Services - Minor	Minor	SSL,FTP,WORM,GOPHER	Dynamic Group	No	Pre-defined
Additional Web Services - Warning	Warning	SSL,FTP,WORM,GOPHER	Dynamic Group	No	Pre-defined
All Attacks			Static Group	No	Pre-defined
Anomaly			Static Group	No	Pre-defined
Anomaly - All			Dynamic Group	No	Pre-defined
Anomaly - Critical	Critical		Dynamic Group	No	Pre-defined
Anomaly - Info	Info		Dynamic Group	No	Pre-defined
Anomaly - Major	Major		Dynamic Group	No	Pre-defined
Anomaly - Minor	Minor		Dynamic Group	No	Pre-defined
Anomaly - Warning	Warning		Dynamic Group	No	Pre-defined
APP		APP	Static Group	No	Pre-defined
APP - All		APP	Dynamic Group	No	Pre-defined
APP - Critical	Critical	APP	Dynamic Group	No	Pre-defined
APP - Info	Info	APP	Dynamic Group	No	Pre-defined
APP - Major	Major	APP	Dynamic Group	No	Pre-defined
APP - Minor	Minor	APP	Dynamic Group	No	Pre-defined

### 3. Click **Create IPS Signature**.

The **Create IPS Signature** page appears, as shown in [Figure 90](#) on page 186.

Figure 90: Create IPS Signature Page

4. Enter the name of the signature in the **Name** field.
5. Enter the category of the signature in the **Category** field.
6. Select the **Recommended** check box if you want this to be a recommended signature.
7. Enter some keywords in the **Keywords** field.
8. Select the appropriate severity of the signature from the **Severity** drop-down menu.
9. Select the appropriate action for the signature from the **Action** drop-down menu.
10. Enter the description for this signature in the **Description** field.

11. Select the **Signature Details** tab from the **Pattern Set** page. Enter the following:
  - a. Select the appropriate option from the **Attack Object Binding** drop-down menu.
  - b. Select the appropriate option from the **Time Scope** drop-down menu.
  - c. Select the appropriate option from the **Match Assurance** drop-down menu.
  - d. Enter the name of the protocol in the **Protocol** field.
  - e. Enter the value of the time count in the **Time Count** field.
  - f. Select the **Performance Impact** check box if you want to do so.
  - g. Click the **Add Signature** button.
  - h. Select the appropriate option from the **Context** drop-down menu.
  - i. Select the appropriate direction from the **Direction** dropdown menu.
  - j. Enter appropriate information in the **Pattern** field.
  - k. Enter appropriate information in the **Regex** field.
  - l. Select the **Negated** check box if you want to do so.
  - m. Select the **Shellcode** check box if you want to do so.
  - n. Click the **Add Anomaly** button.
  - o. Select the appropriate anomaly from the **Anomaly** drop-down menu.
12. Click the **Supported Detectors** button to view the descriptors that are supported with this signature.
13. Click **Save**.

**Related Documentation**

- [Managing IPS Signatures on page 187](#)

## Managing IPS Signatures

You can filter, modify, or delete IPS signatures listed in the **View All IPS Signatures** page.

To open the **View All IPS Signatures** page:

- From the **Security Design** task ribbon, select **IPS Management > IPS Signatures**.

The **View All IPS Signatures** page appears.

You can either right-click or use the Actions drawer to manage IPS signatures.

You can perform the following tasks in the **View All IPS Signatures** page:

- [Filtering IPS Signatures on page 188](#)
- [Modifying IPS Signatures on page 188](#)

- [Deleting IPS Signatures on page 188](#)
- [Cloning IPS Signatures on page 189](#)
- [Creating Static Signature Groups on page 189](#)
- [Creating Dynamic Signature Groups on page 190](#)
- [Creating IPS Signature-sets on page 190](#)

## Filtering IPS Signatures

To filter IPS signatures:

1. From the **Security Design** task ribbon, select **IPS Management > IPS Signatures**.

The **View All IPS Signatures** page displays all IPS signatures. The right pane displays the signatures and the left pane displays the different filters that can be used to filter the signatures. The different parameters that can be used to filter the signatures include, Severity, Category, Object Type, Direction, Action, Match Assurance, Recommended, and Signature Set. Every parameter has different subparameters.

2. Click the check box next to the subparameters within a parameter.

The IPS signatures will now be filtered by the filters you have applied.

## Modifying IPS Signatures

To modify IPS signatures:

1. From the **Security Design** task ribbon, select **IPS Management > IPS Signatures**.

The **View All IPS Signatures** page displays all IPS signatures.

2. Select the check box next to the IPS signature you want to modify.



**NOTE:** You cannot modify a predefined IPS signature. You can only modify the custom IPS signatures you have added.

3. Click **Modify IPS Signature** in the Actions drawer.

You are redirected to the **Modify IPS Signature** page. You can make necessary changes to the application signature here.

4. Click **Save**.

## Deleting IPS Signatures

To delete IPS signatures:

1. From the **Security Design** task ribbon, select **IPS Management > IPS Signatures**.

The **View All IPS Signatures** page displays all IPS signatures.

2. Select the check box next to the IPS signatures you want to delete.



**NOTE:** You cannot delete the predefined IPS signatures. You can only delete the custom IPS signatures you have added.

3. Click **Delete Selected** in the Actions drawer.

A confirmation window appears.

4. Click **Yes**.

## Cloning IPS Signatures

To clone IPS signatures:

1. From the **Security Design** task ribbon, select **IPS Management > IPS Signatures**.

The **View All IPS Signatures** page displays all IPS signatures that are downloaded.

2. Select the check box next to the IPS signature you want to clone.
3. Click **Clone IPS Signature** in the Actions drawer.

You are redirected to the **Create IPS Signature** page. You can clone the IPS signature here.

## Creating Static Signature Groups

To create a static signature group:

1. From the **Security Design** task ribbon, select **IPS Management > IPS Signatures**.

The **View All IPS Signatures** page displays all IPS signatures.

2. Select the check box next to the IPS signatures you want to include in the IPS signature static group.
3. Select **Create Static Group** from the Actions drawer.

The **Create IPS Signature Static Group** page appears.

4. Enter the name of the static signature group in the **Name** field.
5. Select the **Recommended** check box if you want to do so.
6. Click the Add icon to add IPS signatures to the static group.

The **IPS Signature Selector** window appears.

7. Select the appropriate IPS signatures and click **Update**.

## Creating Dynamic Signature Groups

To create a dynamic signature group:

1. From the **Security Design** task ribbon, select **IPS Management > IPS Signatures**.  
The **View All IPS Signatures** page displays all IPS signatures.
2. Select **Create Dynamic Group** from the Actions drawer.  
The **Create IPS Signature Dynamic Group** page appears.
3. Enter the name of the dynamic signature group in the **Name** field.
4. Select the check box next to the appropriate option in the **Recommended** pane.
5. Select the check boxes next to the appropriate actions in the **Actions** pane.
6. Select the appropriate directions from the drop-down menus in the **Direction** pane.
7. Select the appropriate check box in the **Pre-defined/Custom** pane.
8. Select the appropriate check boxes in the **Match Assurance** pane.
9. Select the appropriate check boxes in the **Performance Impact** pane.
10. Click the **Advanced** tab.
11. In the **Category** pane, select the appropriate signatures from the **Available** column and click the right arrow to push them to the **Selected** column.
12. In the **Service** pane, select the appropriate signatures from the **Available** column and click the right arrow to push them to the **Selected** column.
13. Select the appropriate check boxes in the **Severity** pane.
14. Click the **Space Filters** tab.
15. Select the appropriate check boxes in the **Object Type** pane.
16. Select the appropriate check boxes in the **Platform** pane.
17. Enter a name for the vendor in the **Vendor** field.
18. Select the appropriate check boxes in the **Version Changes** pane.
19. Select the appropriate dates from the **Activation Date** pane.
20. Select the appropriate dates from the **Modify Date** pane.
21. Enter an appropriate value in the **in** field in the **Latest Changes** pane.
22. Click **Create**.

## Creating IPS Signature-sets

To create an IPS signature-set:

1. From the **Security Design** task ribbon, select **IPS Management > IPS Signatures**.  
The **View All IPS Signatures** page displays all IPS signatures.



2. Select the appropriate IPS signatures and then click **Create IPS Signature-Set**.

## Creating IPS Signature Sets

To create an IPS signature-set:

1. From the **Security Design** task ribbon, select **IPS Management**.

You see the IPS Policies Tabular view.

2. Click **IPS Signature-Set**.

You see the IPS signature-set Tabular view with two panes and the first signature-set is selected by default. The left pane displays all the IPS signature-sets in the system. The right pane displays all the rules in a specific IPS signature-set as shown in [Figure 91 on page 191](#).

Figure 91: IPS Signature Set Tabular View

Rule Type	IPS Signature	Action	Notification	IP Action	Additional	Description
IPS	[Recommended]IP - Critical [Recommended]IP - Minor [Recommended]IP - Major [Recommended]IP - Critical More +	Recommended		IP Action: None IP Target: None Timeout: 0 Log IP Action: Disable	Severity: None Terminal: Disable	This rule is designed to protect your network against important TCP/IP attacks.
IPS	[Recommended]ICMP - Major [Recommended]ICMP - Minor	Recommended		IP Action: None IP Target: None Timeout: 0 Log IP Action: Disable	Severity: None Terminal: Disable	This rule is designed to protect your network against important ICMP attacks.
IPS	[Recommended]HTTP - Critical [Recommended]HTTP - Major [Recommended]HTTP - Minor	Recommended		IP Action: None IP Target: None Timeout: 0 Log IP Action: Disable	Severity: None Terminal: Disable	This rule is designed to protect your network against important HTTP attacks.
IPS	[Recommended]SMTP - Critical [Recommended]SMTP - Major [Recommended]SMTP - Minor	Recommended		IP Action: None IP Target: None Timeout: 0 Log IP Action: Disable	Severity: None Terminal: Disable	This rule is designed to protect your network against important SMTP attacks.
IPS	[Recommended]DNS - Critical [Recommended]DNS - Minor [Recommended]DNS - Major	Recommended		IP Action: None IP Target: None Timeout: 0 Log IP Action: Disable	Severity: None Terminal: Disable	This rule is designed to protect your network against important DNS attacks.
IPS	[Recommended]FTP - Critical [Recommended]FTP - Minor [Recommended]FTP - Major	Recommended		IP Action: None IP Target: None Timeout: 0 Log IP Action: Disable	Severity: None Terminal: Disable	This rule is designed to protect your network against important FTP attacks.
IPS	[Recommended]POP3 - Critical [Recommended]POP3 - Minor [Recommended]POP3 - Major	Recommended		IP Action: None IP Target: None Timeout: 0 Log IP Action: Disable	Severity: None Terminal: Disable	This rule is designed to protect your network against important POP3 attacks.
IPS	[Recommended]IMAP - Critical			IP Action: None IP Target: None	Severity: None	This rule is designed to protect your network

All the IPS signature-sets under the **Predefined** node are predefined signature sets. All the IPS signature-sets under the **Custom** node are user-defined signature sets.

3. Click **Create IPS Signature-Set**.

The **Create IPS Signature-Set** page appears.

4. Enter the name of the IPS signature-set in the **Name** field.
5. Enter the name for the IPS signature-set in the **Description** field.
6. Click **Create**.

### Related Documentation

- [Adding Rules to an IPS Signature Set on page 192](#)
- [Managing IPS Signature Sets on page 193](#)

## Adding Rules to an IPS Signature Set

---

To add rules to an IPS signature-set:

1. From the **Security Design** task ribbon, select **IPS Management > IPS Signature-Set**.

The IPS signature-set Tabular view appears.

2. Click the IPS signature-set you want to add rules to from the left pane.

The existing rules of the IPS signature-set are displayed in the right pane.

3. Click the **Add Rule** icon and select the type of the rule you want to add.

A new rule is added in the bottom-most row.

4. Click the **IPS Signature** column in the rule.

The **IPS Signature Selector** window appears. You can select and add IPS signatures from this window.

5. Click **Update** in the **IPS Signature Selector** window when you select the IPS signatures for the rule.

6. Click the **Action** column in the rule and select the appropriate action for the rule.

7. Click the **Notification** column in the rule.

A drop-down menu with all notification options appears. To add appropriate notification options:

- a. Click the **Enable** check box next to the **Attack Logging** field if you want to log the attacks.
- b. Click the **Enable** check box next to the **Attack Flag** field if you want to flag attacks.
- c. Select the appropriate option from the **IP Action** drop-down menu.
- d. Select the appropriate option from the **IP Target** drop-down menu.
- e. Enter the value of the timeout interval in the **Timeout** field.
- f. Click the **Enable** check box next to the **Log IP Action** field if you want to maintain a log of the IP actions performed.
- g. Select the appropriate severity from the **Severity** drop-down menu.
- h. Click the **Enable** check box next to **Terminal** field.
- i. Click **Update**.



**NOTE:** You can also modify the IP action and the additional sections in the **Notification** drop-down menu by clicking the **IP Action** and **Additional** columns in the rule.

---

8. Click the **Description** column and enter a description for the rule.
9. Click **Save**.

**Related  
Documentation**

- [Creating IPS Signature Sets on page 191](#)
- [Managing IPS Signature Sets on page 193](#)

## Managing IPS Signature Sets

- [Deleting IPS Signature-sets on page 193](#)
- [Cloning IPS Signature-sets on page 193](#)
- [Enable or Disable Rules in an IPS Signature-set on page 194](#)

### Deleting IPS Signature-sets

To delete an IPS signature-sets:

1. From the **Security Design** task ribbon, select **IPS Management > IPS Signature-Set**.

The **IPS Signature Set** page displays all signature sets. The left pane displays the predefined and custom signature sets. The right pane displays the signatures in the respective signature-set.

2. Right-click the signature-set you want to delete and select **Delete IPS Signature Set**.

A confirmation window appears.



**NOTE:** You cannot delete a predefined signature-set. You can only delete a custom signature-set.

3. Click **Yes**.

### Cloning IPS Signature-sets

To clone an IPS signature-sets:

1. From the **Security Design** task ribbon, select **IPS Management > IPS Signature-Set**.

The **IPS Signature Set** page displays all signature-sets. The left pane displays the predefined and custom signature sets. The right pane displays the signatures in the respective signature-set.

2. Right-click the signature-set you want to clone and select **Clone IPS Signature Set**.

You are redirected to the **Clone IPS Signature Set** page. You can modify the name and description on this page.

3. Click **Clone**.

## Enable or Disable Rules in an IPS Signature-set

To enable or disable rules in an IPS signature-set:

1. From the **Security Design** task ribbon, select **IPS Management > IPS Signature-Set**.

The **IPS Signature Set** page displays all signature-sets. The left pane displays the predefines and custom signature-sets. The right pane displays the signatures in the respective signature-set.

2. Select the signature-set for which you want to enable or disable the rule in the left pane.

All rules of the this signature-set appear in the right pane.

3. Select the rule you want to enable or disable and click the appropriate button.

The disabled rule appears dimmed.

4. Click **Save**.

## Creating IPS Policies

You can create IPS policies only if you set the IPS configuration mode to Manual in the device firewall policy. If you want to enable IPS policy creation for a group firewall policy, you would need to:

- Enable IPS configuration mode to Manual for the devices in the group firewall policy.
- Set the **Action** field for the device rule for which you want to enable the firewall policy to **Permit**.
- Select the appropriate IPS signature set in the IPS field of the device rule.

To create an IPS policy from the firewall policy:

- Set the IPS configuration mode to Manual.
- In the firewall policy tabular view, set IPS to IPS ON. An empty container is created in the right pane as shown [Figure 92 on page 195](#).

**Figure 92: IPS Management Right Pane View**

Name	Rule Type	Source		Destination		Service	IPS Signature	Action	Notification	IPS Options
		Zone	Address	Zone	Address					
<a href="#">New IPS</a> <a href="#">New Exempt</a>										
1	IPS	Any	Any	Any	Any	Default	None	Recommended		IP Action: None IP Target: None Timeout: 0 Log IP Action: Dis
2	Exempt	Any	Any	Any	Any	Default	None			

- Click **New IPS** to add new policy rules and **New Exempt** to add new exempt rules.

To create an IPS policy:

1. From the **Security Design** task ribbon, select **IPS Management**.

The IPS Policies Tabular view appears. The left pane of this Tabular view displays the firewall policies and the right pane displays the all devices policy rules and the device rules for which IPS policy can be created as shown in [Figure 93 on page 196](#).

**Figure 93: IPS Policies Tabular View**

Rule Type	Zone	Source Address	Destination Zone	Destination Address	Service	IPS Signature	Action	Notification
test1 - Pre Rules - test1-Pre-1 - Recommended (5 Rules)								
IPS	Any	Any	Any	Any	Default	[Recommended]IP - Critical [Recommended]IP - Minor [Recommended]IP - Major [Recommended]TCP - Critical	Recommended	
IPS	Any	Any	Any	Any	Default	[Recommended]SSH - Major [Recommended]SSH - Minor	Recommended	
IPS	Any	Any	Any	Any	Default	[Recommended]HTTP - Critical [Recommended]HTTP - Major [Recommended]HTTP - Minor	Recommended	
IPS	Any	Any	Any	Any	Default	[Recommended]SMTP - Critical [Recommended]SMTP - Major [Recommended]SMTP - Minor	Recommended	
IPS	Any	Any	Any	Any	Default	[Recommended]DNS - Critical [Recommended]DNS - Minor [Recommended]DNS - Major	Recommended	
IPS	Any	Any	Any	Any	Default	[Recommended]FTP - Critical [Recommended]FTP - Minor [Recommended]FTP - Major	Recommended	
IPS	Any	Any	Any	Any	Default	[Recommended]POP3 - Critical [Recommended]POP3 - Minor	Recommended	

2. Select the device policy for which you want to create an IPS policy.

The right pane displays the device policy for which the IPS policy can be created.



**NOTE:** You will see all devices policy rules and device rules for which the **Action** field is set to **Permit** and an appropriate IPS signature-set is selected in the right pane.

3. Select the IPS signature in the IPS signature-set that you want to customize for creating an IPS policy and modify the fields appropriately.

You can now add more IPS and exempt rules for this device rule.

4. Click the **Add Rule** icon and select the type of the rule you want to add.

A new rule is added in the bottom-most row. If you add an IPS rule, by default, the Source and Destination zones and addresses are inherited from the device rule. The **IPS Signature** field is set to **None**. You can now customize the fields in this rule.

For logical systems, you cannot edit source and destination zones, source and destination addresses, and application. Automatically, Security Design sets zone and address fields as 'Any' and application field as 'default'.

5. Click **Save**.

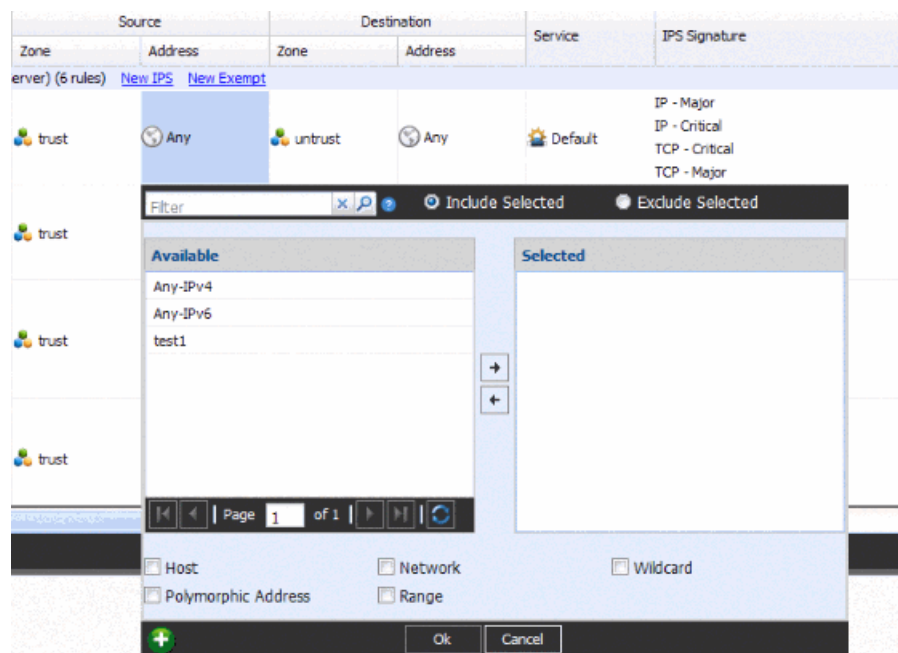


**NOTE:** When the firewall policy is published and updated on the device, the IPS policy configuration is also pushed along with the firewall configuration.

To create address objects for the IPS policy:

1. Click on the source address. The Create IPS Policy Objects page, as shown in [Figure 94 on page 197](#) appears. The page lists the addresses available for creating the objects.

**Figure 94: Create IPS Policy Address Objects Page**



2. Click the plus sign (+) to create the new address object for the IPS policy.

**Figure 95: Create IPS Policy Address Page**

3. Click **Create** to create the new address object, or click **Cancel** to discard all changes.

**Related Documentation**

- [Publishing IPS Policies on page 198](#)
- [Managing IPS Policies on page 201](#)

## Publishing IPS Policies

To publish an IPS policy:

1. From the **Security Design** taskbar, select **IPS Management > Publish IPS Policy**.

The **Services** page appears with all the IPS policies. It also displays the publish states of the IPS policies.

2. Select the check box next to the IPS policy that you want to publish.



**NOTE:** You can search for a specific device on which the policy is published by entering the search criteria in the Search field, on the right top corner of the **Services** page. You can search the devices by their name, IP address, and device tags.



**NOTE:** If the IPS policy is to be published on a large number of devices, the devices are displayed across multiple pages. You can use the pagination and display options available on the lower ribbon, just below the list of devices, to view all devices on which the policy is published.

3. Select the **Schedule at a later time** check box if you want to schedule and publish the configuration later, as shown in [Figure 96 on page 198](#).

Figure 96: IPS Policy Publish Page

Name	Publish State	Description
<input type="checkbox"/> Global Policy	Not Published	Predefined Global Policy
<input type="checkbox"/> test-pubs	Not Published	
<input checked="" type="checkbox"/> test-pubs	Not Published	
<input type="checkbox"/> x1	Re-publishing Required	

☐ Schedule at a later time

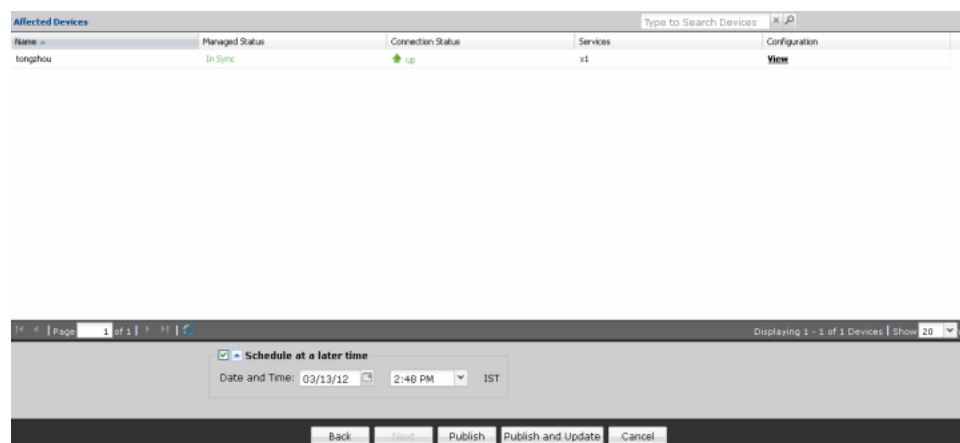
Back Next Publish Publish and Update Cancel

4. Click **Next**.

The **Affected Devices** page displays the devices on which this IPS policy will be published, as shown in [Figure 97 on page 199](#).



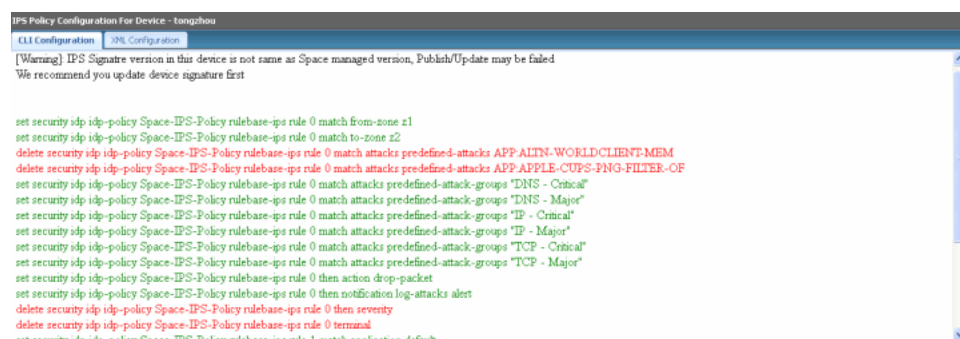
Figure 97: Policy Publish: Affected Devices Page



5. If you want to preview the configuration changes that will be pushed to the device, click the **View** link in the **Configuration** column that corresponds to the device. A **Configuration Preview** progress bar is shown while the configuration to be pushed to the device is generated.

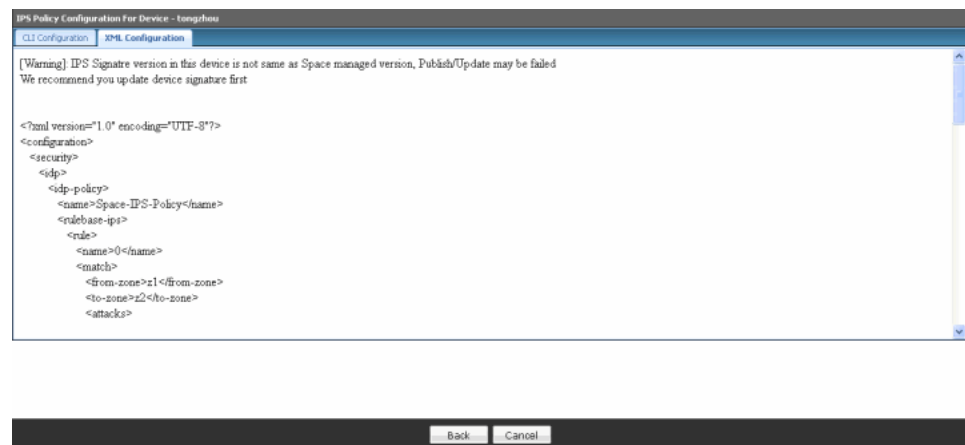
The **CLI Configuration** tab appears by default. You can view the configuration details in CLI format, as shown in [Figure 98 on page 199](#).

Figure 98: Policy Publish: CLI Configuration



6. View the XML format of the configuration by clicking the **XML Configuration** tab, as shown in [Figure 99 on page 200](#).

Figure 99: Policy Publish: XML Configuration



7. Click **Back**.

8. Click **Publish** if you want only to publish the configuration.

A new job is created and the job ID appears in the **Job Information** dialog box.

9. Click **Publish and Update** if you want both to publish and to update the devices with the configuration.

The IPS policy is now moved into the Published state if the configuration is published to all devices involved in the IPS policy. If the configuration is not published to all devices involved in the IPS policy, the IPS policy is placed in the Partially Published state. If an IPS policy is created but not published, the IPS policy is placed in the Unpublished state. If any modifications are made to IPS policy configuration after it is published, the IPS policy is placed in the Republish Required state. You can view the states of the policies by hovering over them.

A new job is created and the job ID appears in the **Job Information** dialog box.

10. Click the job ID to view more information about the job created. This action redirects you to the **Job Management** workspace.

If you get an error message during the publish, or if the IPS policy publish fails, go to the Job Management workspace and view the relevant job ID to see why the publish failed.



**NOTE:** You can also publish an IPS policy by right-clicking the IPS policy in the IPS Policy Tabular view and selecting **Publish Policy**. You are redirected to the **Affected Devices** page.

#### Related Documentation

- [Creating IPS Policies on page 195](#)
- [Managing IPS Policies on page 201](#)

## Managing IPS Policies

---

You can delete, enable, and disable rules in an IPS policy.

To open the **IPS Policies** page:

- From the **Security Design** task ribbon, select **IPS Management**.

The IPS Policy Tabular view appears.

You can perform the following tasks in the **IPS Policies** space:

1. [Deleting IPS Policy Rules on page 201](#)
2. [Enabling or Disabling Rules in an IPS Policy on page 201](#)

### Deleting IPS Policy Rules

To delete rules in an IPS policy:

1. From the **Security Design** task ribbon, select **IPS Management**.

The IPS Policy Tabular view appears.

2. Select the device policy from which you want to delete IPS policy rules.

The right pane displays the device rules for which IPS policy is enabled.

3. Select the check box next to the IPS or exempt rule you want to delete.
4. Click the Delete icon.
5. Click **Save**.

### Enabling or Disabling Rules in an IPS Policy

To enable or disable rules in an IPS policy:

1. From the **Security Design** task ribbon, select **IPS Management**.

The IPS Policy Tabular view appears.

2. Select the firewall policy whose IPS rules you want to enable or disable.

The rules of the firewall policy are displayed in the right pane.

3. Select the check boxes next to the rules that you want to enable or disable.
4. Click the **Enable** or **Disable** icon.
5. Click **Save**.



## PART 10

# Security Design Devices

- [Security Design Devices on page 205](#)



## CHAPTER 22

# Security Design Devices

- Updating Devices with Pending Services on page 205
- Importing Firewall and NAT Policies from a Device to Security Design on page 207
- NSM Migration on page 211

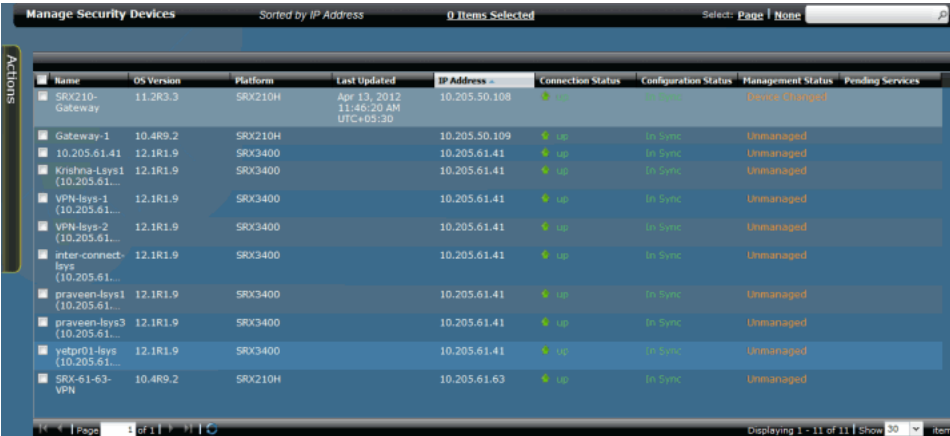
## Updating Devices with Pending Services

To update a device with pending services:

1. From the **Security Design** task ribbon, select **Security Design Devices**.

The **Manage Security Devices** page appears, as shown in Figure 100 on page 205.

Figure 100: Security Design Devices Page

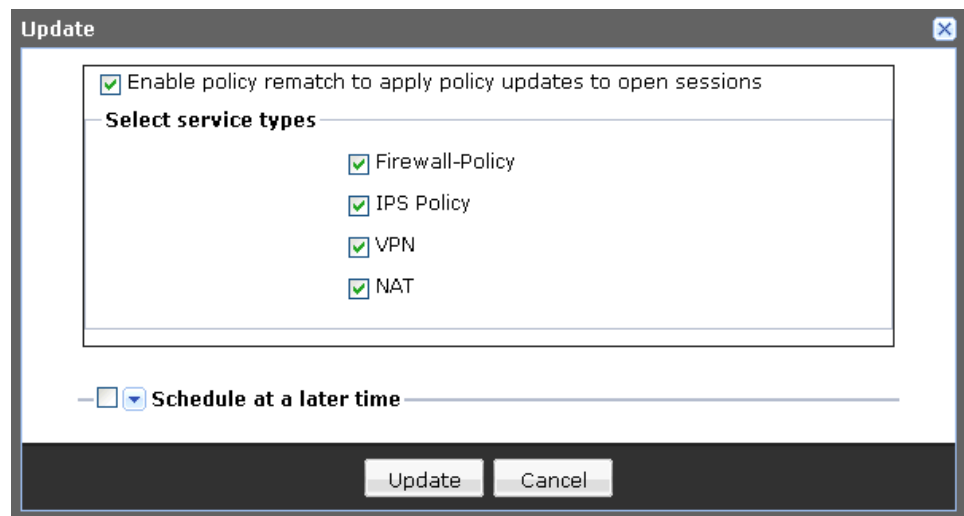


Name	OS Version	Platform	Last Updated	IP Address	Connection Status	Configuration Status	Management Status	Pending Services
SRX210-Gateway	11.2R3.3	SRX210H	Apr 13, 2012 11:46:20 AM UTC+05:30	10.205.50.108	Up	In Sync	Device Changed	
Gateway-1	10.4R9.2	SRX210H		10.205.50.109	Up	In Sync	Unmanaged	
10.205.61.41	12.1R1.9	SRX3400		10.205.61.41	Up	In Sync	Unmanaged	
Krishna-Isys1 (10.205.61...	12.1R1.9	SRX3400		10.205.61.41	Up	In Sync	Unmanaged	
VPN-Isys-1 (10.205.61...	12.1R1.9	SRX3400		10.205.61.41	Up	In Sync	Unmanaged	
VPN-Isys-2 (10.205.61...	12.1R1.9	SRX3400		10.205.61.41	Up	In Sync	Unmanaged	
inter-connect-Isys (10.205.61...	12.1R1.9	SRX3400		10.205.61.41	Up	In Sync	Unmanaged	
praveen-Isys1 (10.205.61...	12.1R1.9	SRX3400		10.205.61.41	Up	In Sync	Unmanaged	
praveen-Isys3 (10.205.61...	12.1R1.9	SRX3400		10.205.61.41	Up	In Sync	Unmanaged	
yelp01-Isys (10.205.61...	12.1R1.9	SRX3400		10.205.61.41	Up	In Sync	Unmanaged	
SRX-61-63-VPN	10.4R9.2	SRX210H		10.205.61.63	Up	In Sync	Unmanaged	

2. Select the check box next to the device on which you want to update the pending services.
3. Click **Update**.

The **Update** page appears, as shown in Figure 101 on page 206.

Figure 101: Update Window



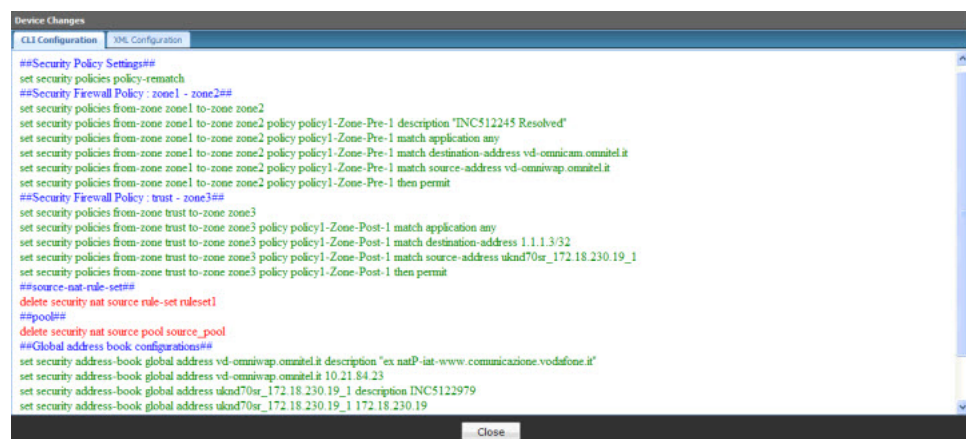
4. Select the type of service you want to update on the device in **Select Service Types** pane.
5. Select the **Schedule at a later time** check box if you want to schedule the update at a later date and time.
6. Click **Update**.

To view the description entered for the device:

1. In the **Manage Security Devices** page, right-click on the device for which policies are published, and select **Preview Configuration**.
2. The **Preview Configuration** window appears. Select the service type and click **OK**.

The publish window appears showing the descriptions for the policy rules and objects in the CLI to be pushed to the device, as shown in [Figure 102 on page 206](#).

Figure 102: Device Changes Page Showing Device Comments







**NOTE:** Description entered for the address or service or NAT pool objects used in the firewall or NAT policies, and description for NAT or firewall policy rules, are also pushed to the device. This feature is supported for the devices running Junos OS Release 12.1 and later.

## Importing Firewall and NAT Policies from a Device to Security Design

Security Design enables you to import firewall and NAT policies from a device. All objects supported by Security Design are imported during the policy import process. Rules that contain objects not supported by Security Design are imported with the disabled rule state.

You can select a list of policies to be imported to Security Design. Security Design displays a summary of the rules and objects used in the policies to be imported. After you verify the information and resolve any conflicts, the policies are imported from the device to Security Design. Every time a new import is initiated, Security Design creates a new policy, even if a policy with that name was imported previously. In such a case, Security Design names the new policy based on the results of the duplicate name resolution.



**NOTE:** Imported policies are created without any device assigned to them and for using these policies, you must associate a device with the policy

To import a firewall or NAT policy:

1. From the **Security Design** taskbar, select **Security Design Devices**.

The **Manage Security Devices** page appears, as shown in [Figure 103 on page 207](#).

**Figure 103: Manage Security Devices Page**

Name	OS Version	Platform	Last Updated	IP Address	Connection Status	Configuration Status	Management Status	Pending Services
SRX210-Gateway	11.2R3.3	SRX210H	Apr 13, 2012 11:46:20 AM UTC+05:30	10.205.50.108	Up	In Sync	Device Changed	
Gateway-1	10.4R9.2	SRX210H		10.205.50.109	Up	In Sync	Unmanaged	
10.205.61.41	12.1R1.9	SRX3400		10.205.61.41	Up	In Sync	Unmanaged	
KmPaaS-Lys1 (10.205.61...	12.1R1.9	SRX3400		10.205.61.41	Up	In Sync	Unmanaged	
VPN-lys-1 (10.205.61...	12.1R1.9	SRX3400		10.205.61.41	Up	In Sync	Unmanaged	
VPN-lys-2 (10.205.61...	12.1R1.9	SRX3400		10.205.61.41	Up	In Sync	Unmanaged	
inter-connect-lys (10.205.61...	12.1R1.9	SRX3400		10.205.61.41	Up	In Sync	Unmanaged	
praveen-lys1 (10.205.61...	12.1R1.9	SRX3400		10.205.61.41	Up	In Sync	Unmanaged	
praveen-lys3 (10.205.61...	12.1R1.9	SRX3400		10.205.61.41	Up	In Sync	Unmanaged	
yotpr01-lys (10.205.61...	12.1R1.9	SRX3400		10.205.61.41	Up	In Sync	Unmanaged	
SRX-61-63-VPN	10.4R9.2	SRX210H		10.205.61.63	Up	In Sync	Unmanaged	

2. Select the device for which you want to import the policy. Right-click on the device, and then click **Import**.

The **Service Import Summary** page appears, as shown in [Figure 104 on page 208](#).

Figure 104: Service Import Summary Page

Policy	Rules	Errors	Summary
NAT Policies	1	0	
Firewall Policies	36	0	

This page provides the following information:

- Policy name and type ( firewall or NAT)
- Number of rules with errors or warnings
- Summary showing:
  - Number of addresses, services, or NAT pool objects
  - Rules with unsupported objects

3. Select the policy that you want to import, and click **Next**.

If conflicts are present, the, **Object Conflict Resolution** page appears, as shown in [Figure 105 on page 208](#).

Figure 105: Object Conflict Resolution Page for Firewall Policy

Name	Value	Imported value	Action	New Name
QOS_HIGHT	[QATF_HIGHT, QATF_HIGHT2, QOS_HIGHT1, QOS_HIGHT2, QOS_HIGHT3, QOS_HIGHT4]	[QOS_HIGHT1, QOS_HIGHT2, QOS_HIGHT3, QOS_HIGHT4]	Rename Object	QOS_HIGHT_1
QOS_HIGHT_1	[QATF_HIGHT, QATF_HIGHT2, QOS_HIGHT2, QOS_HIGHT3, QOS_HIGHT4]	[QOS_HIGHT2, QOS_HIGHT3, QOS_HIGHT4]	Rename Object	QOS_HIGHT_1
QOS_DCL	[aggrdncl1, aggrdncl2, aggrdncl3, aggrdncl4]	[aggrdncl1, aggrdncl2, aggrdncl3, aggrdncl4]	Rename Object	QOS_DCL_1

An object conflict occurs when the name of the object to be imported matches an existing object, but the definition of the object does not match. You can use the available Tooltip view to see more information for Value, Imported Value, and Action columns. To see the tooltip for an object, mouse over its value, imported value, or action columns.

Conflicting objects can be address, service, or NAT pool objects. You can take the following actions for the conflicting objects from the action column:

- Keep the existing object, and ignore the new object.

- Overwrite the existing object with the new object.
- Accept the proposed name, or enter a new name.

Once the initial naming conflict has been resolved, the object conflict resolution checks for further conflicts with the new name and definition until conflict is completely resolved.

4. After all object conflicts are resolved, click **Next**. A summary of the import process appears, along with the conflict resolution page, as shown in [Figure 106 on page 209](#).

**Figure 106: Firewall Policy Import Status Page**

**Print Report**

**Selected Devices**

Name	IP Address	Platform	Software Release	is Cluster
10.205.61.41	10.205.61.41	SRX3400	12.1R1.9	No

**Selected Services**

Type	Name	Policy Type	Total Lines	Errors	Warnings	Summary
Permit	10.205.61.41	Device	30	0	0	
NAT	10.205.61.41	Device	1	0	0	

**Object Error Summary**

Type	Object	Affected Objects	Errors
No Errors			

**Object Conflict Resolution**

Object Type	Old Name	Resolution	Resolved Name
Address	QDR_HQMT_localhosts	Create with New Name	QDR_HQMT_localhosts_1
Address	QSI-OCs	Create with New Name	QSI-OCs_2
Address	QDR_HQMT	Create with New Name	QDR_HQMT_1

Previous Finish Cancel

To print the summary report, click **Print Report** at the beginning of the page.



**NOTE:** If Security Design finds further conflicts, the **Object Conflict Resolution** page is refreshed to display the new conflicts.

5. Click **Finish** to initiate the import process. After the import is complete, a comprehensive report for each policy imported is provided, as shown in [Figure 107 on page 210](#).

Figure 107: Firewall Policy Final Import Status Page



Task	Status	Details
Reading import Files	Inprogress	Started at Wed May 02 06:39:49 UTC 2012
Reading import Files	Success	Finished at Wed May 02 06:39:49 UTC 2012
Import Addresses to Security Design	Inprogress	Importing Started at Wed May 02 06:39:49 UTC 2012
Import Addresses to Security Design	Success	Finished at Wed May 02 06:39:50 UTC 2012
Import Services to Security Design	Inprogress	Started at Wed May 02 06:39:50 UTC 2012
Import Services to Security Design	Success	Finished at Wed May 02 06:39:50 UTC 2012
Import Nat Prefixes to Security Design	Inprogress	Started at Wed May 02 06:39:50 UTC 2012
Import Nat Prefixes to Security Design	Success	Finished at Wed May 02 06:39:51 UTC 2012
Import Nat Pools to Security Design	Inprogress	Started at Wed May 02 06:39:51 UTC 2012
Import Nat Pools to Security Design	Success	Finished at Wed May 02 06:39:51 UTC 2012
Import firewall policy to Security Design	Inprogress	Importing 10.205.61.41 Started at Wed May 02 06:39:51 UTC 2012
Import firewall policy to Security Design	Success	Imported as 10.205.61.41 Finished at Wed May 02 06:39:51 UTC 2012
Import Nat Policy to Security Design	Inprogress	Importing 10.205.61.41 Started at Wed May 02 06:39:51 UTC 2012
Import Nat Policy to Security Design	Success	Imported as 10.205.61.41 Finished at Wed May 02 06:39:51 UTC 2012
Import Summary		<a href="#">Summary Report</a>

Page 1 of 1 | Displaying 1 - 15 of 15

- Click on **Summary Report** to view the import summary as shown in [Figure 106 on page 209](#)
- Go to the firewall policy workspace to view the imported policies. At this point Security Design will have created a device policy without associating any devices with it. At this point you can continue to import policy objects for all other devices as many number of times as required. All imported device policies will show up as device policies.

Go to the NAT policy workspace to view the imported policies. All imported device policies will show up as group policies in Security Design. At this point you can continue to import policy objects for all other devices. You can perform all normal NAT policy functions on these imported policies.

If a device firewall policy is imported to Security Design, it automatically creates rule groups based on the zone pair. If a zone pair contains more than 300 rules, based on the auto group feature, the rule groups are broken into multiple rule groups each containing 200 rules. Group names for such groups are decided based on the following logic:

- <ZONE-NAME>-Intra (in case *from zone* and *to zone* are same)
- <SRX ZONE NAME>-to-<DST ZONE NAME>
- <SRX ZONE NAME>-to-<DST ZONE NAME>-X

X is a counter that allows multiple groups when a policy count exceeds 200.

**NOTE:**

- In Junos OS Release 12.1 and later releases, comments are imported during the policy import process.
- You can also import policies from logical systems similar to other devices.
- The following rules are not supported by NAT. After the import, Security Design will disable these rules.
  - Persistent NAT for source-nat interface
  - Persistent NAT for source-nat pool
  - IPv6 to IPv4 translation with the destination address 2001:470:b:227::1/96
  - Matching Protocol in source and destination rule (supported only from Junos OS Release 11.4 and later releases)
  - Matching address object for source and destination address in source, or destination, or static NAT rules
- Security Design does not assign devices to the imported policies. You must explicitly assign devices once the import is complete.

**Related Documentation**

- [NSM Migration on page 211](#)

## NSM Migration

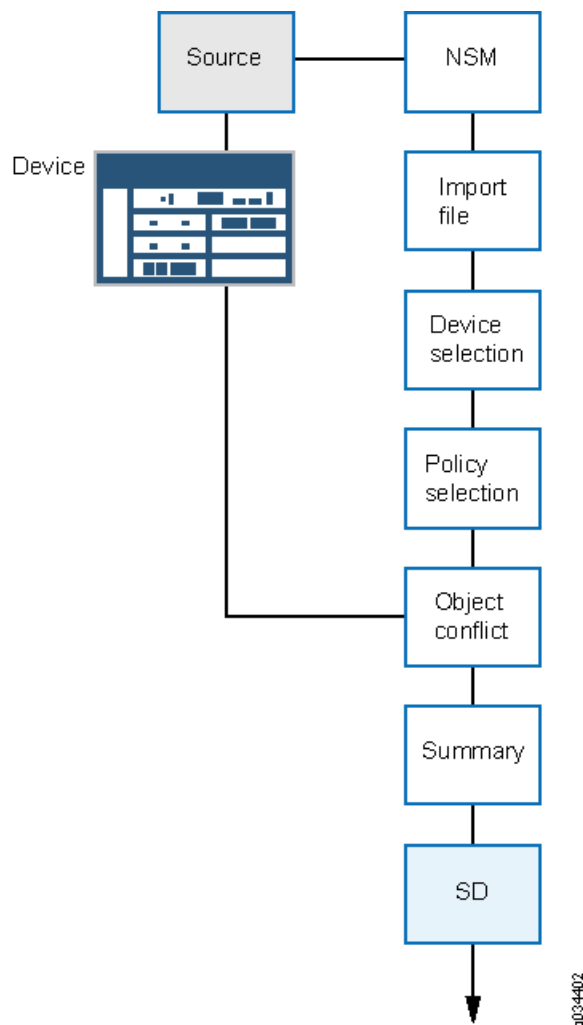
---

You can migrate firewall and NAT policies from Network and Security Manager (NSM) for a set of devices. All objects supported by Security Design (Addresses, Services, Address group, Service group) can be imported with the policy, with the exception of polymorphic objects. Rules referring to these objects are disabled after the migration.

At any time, only a single migrate from the NSM workflow can be triggered on Security Design. Migrating policies from NSM requires the NSM database to be exported in .xdiff format. You must copy this file to your local machine and provide the path of the .xdiff file to migrate policies from NSM to Security Design.

The following [Figure 108 on page 212](#) shows the workflow of device import:

Figure 108: High-level Device Import Workflow

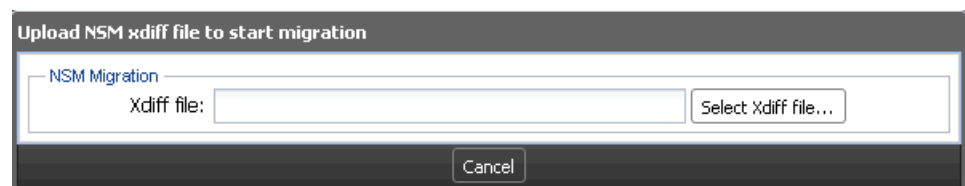


To import policies from NSM:

1. From the **Security Design** taskbar, select **Security Design Devices > NSM Migration**.

The **Upload NSM xdiff file to start migration** window appears, as shown in [Figure 109 on page 212](#).

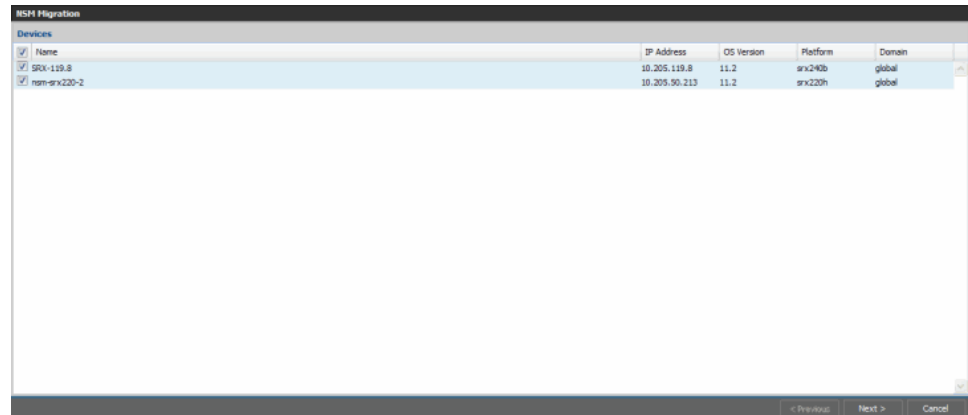
Figure 109: NSM Xdiff File Upload Page



2. Browse to the path where the .xdiff file is stored, and select the appropriate .xdiff file, generated from NSM. The .xdiff file is imported to the Security Design server.

The **Devices** page appears showing the name of the available devices, the Junos OS version of each device, and the platform.

Figure 110: NSM Migration Devices Page

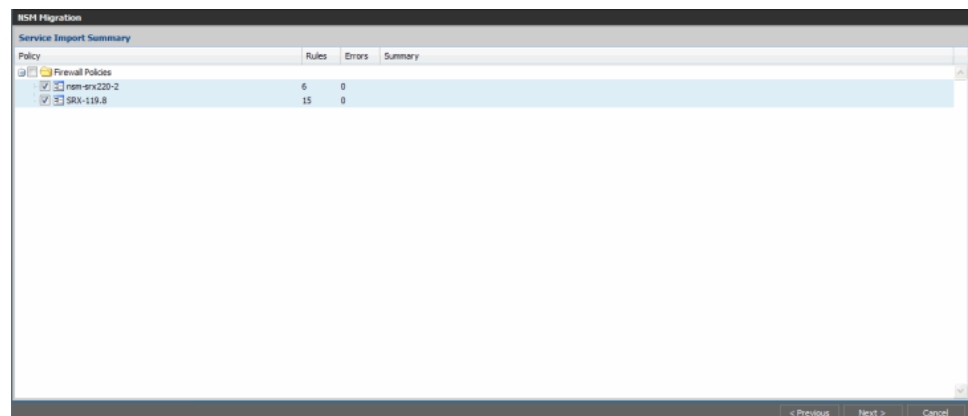


<input checked="" type="checkbox"/>	Name	IP Address	OS Version	Platform	Domain
<input checked="" type="checkbox"/>	SRX-119.8	10.205.119.8	11.2	srx240b	global
<input checked="" type="checkbox"/>	nsn-srx220-2	10.205.90.213	11.2	srx220h	global

3. Select the devices for which you want to import the policies, and select **Next**.

The **Service Import Summary** page appears, as shown in [Figure 111 on page 213](#).

Figure 111: Service Import Summary Page



Policy		Rules	Errors	Summary
<input checked="" type="checkbox"/>	Firewall Policies			
<input checked="" type="checkbox"/>	nsn-srx220-2	6	0	
<input checked="" type="checkbox"/>	SRX-119.8	15	0	

This page provides the following information:

- Policy name and type ( firewall or NAT)
  - Number of rules with errors or warnings
  - Summary showing:
    - Number of addresses, services, or NAT pool objects
    - Rules with unsupported objects (UTM, Scheduler)
4. Select the policy that you want to import, and click **Next**.

If conflicts are present, **Object Conflict Resolution** page appears, as shown in [Figure 112 on page 214](#).

Figure 112: NSM—Object Conflict Resolution Page

Name	Value	Imported Value	Action	New Name
QOL_MGMT	[QATP_MGMT, QATP_MGMT2, QOL_MGMT1, QOL_MGMT2, QOL_MGMT3, QOL_MGMT4]	[QOL_MGMT1, QOL_MGMT2, QOL_MGMT3, QOL_MGMT4]	Rename Object	QOL_MGMT_1
QOL_MGMT_inspacks	[QATP_MGMT, QATP_MGMT2, QOL_MGMT2, QOL_MGMT3, QOL_MGMT4]	[QOL_MGMT1, QOL_MGMT2, QOL_MGMT4]	Rename Object	QOL_MGMT_inspacks_1
QOL-DCs	[aggrdncl1, aggrdncl2, aggrdncl3, aggrdncl4]	[aggrdncl1, aggrdncl2, aggrdncl3, aggrdncl4]	Rename Object	QOL-DCs_1

**QOL-DCs**

Source: Existing    Address Book: QOL\_Outside

Members:	Members:
aggrdncl1	aggrdncl1
aggrdncl2	aggrdncl2
aggrdncl3_1	aggrdncl3
aggrdncl4	aggrdncl4

An object conflict occurs when the name of the object to be imported matches an existing object, but the definition of the object does not match.

Conflicting objects can be address, service, or NAT pool objects. You can take the following actions for the conflicting objects from the action column:

- Keep the existing object, and ignore the new object.
- Overwrite the existing object with the new object.
- Accept the proposed name, or enter a new name.

Once the initial naming conflict has been resolved, the object conflict resolution checks for further conflicts with the new name and definition until resolution is complete.

- After all object conflicts are resolved, click **Next**. A summary of the import process appears, along with the conflict resolution page, as shown in [Figure 113 on page 214](#).

Figure 113: NSM Migration Status Page

**Print Report**

**Managed Devices**

Name	IP Address	Platform	Software Release	Domain name	Is Cluster
SRX-119.8	10.205.119.8	srx240b	11.2	global	No
mem-srx220-2	10.205.50.213	srx220h	11.2	global	No

**Managed Services**

Type	Name	Policy Type	Total Lines	Errors	Warning	Summary
Firewall	mem-srx220-2	Group	6	0	0	
Firewall	SRX-119.8	Group	15	0	0	

**Object Error Summary**

Type	Object	Affected Objects	Errors
No Errors			

**Object Conflict Resolution**

Object Type	Old Name	Resolution	Resolved Name
No Conflicts			

To print the summary report, click **Print Report** at the beginning of the page.



**NOTE:** If Security Design finds further conflicts, the **Object Conflict Resolution** page is refreshed to display the new conflicts..



6. Click **Finish** to initiate the import process.. After the import is complete, a comprehensive report for each policy imported is provided, as shown in [Figure 114 on page 215](#).

Figure 114: NSM Migration Final Status Report Page

Task	Status	Details
Reading import Files	Inprogress	Started at Wed May 02 06:57:37 UTC 2012
Reading import Files	Success	Finished at Wed May 02 06:57:37 UTC 2012
Import Addresses to Security Design	Inprogress	Importing Started at Wed May 02 06:57:37 UTC 2012
Import Addresses to Security Design	Success	Finished at Wed May 02 06:57:38 UTC 2012
Import Services to Security Design	Inprogress	Started at Wed May 02 06:57:38 UTC 2012
Import Services to Security Design	Success	Finished at Wed May 02 06:57:38 UTC 2012
Import Nat Prefixes to Security Design	Inprogress	Started at Wed May 02 06:57:38 UTC 2012
Import Nat Prefixes to Security Design	Success	Finished at Wed May 02 06:57:38 UTC 2012
Import Nat Pools to Security Design	Inprogress	Started at Wed May 02 06:57:38 UTC 2012
Import Nat Pools to Security Design	Success	Finished at Wed May 02 06:57:38 UTC 2012
Import firewall policy to Security Design	Inprogress	Importing nsm-srx220-2 Started at Wed May 02 06:57:38 UTC 2012
Import firewall policy to Security Design	Success	Imported as nsm-srx220-2 Finished at Wed May 02 06:57:39 UTC 2012
Import firewall policy to Security Design	Inprogress	Importing SRX-119.8 Started at Wed May 02 06:57:39 UTC 2012
Import firewall policy to Security Design	Success	Imported as SRX-119.8 Finished at Wed May 02 06:57:39 UTC 2012
Import Summary		<a href="#">Summary Report</a>

7. Click on **Summary Report** to view the import summary as shown in [Figure 113 on page 214](#)
8. Go to the firewall policy or NAT policy workspace to view the imported policies. At this point Security Design will have created a group policy without associating any devices with it. At this point you can continue to import policy objects for all other devices. All imported device policies will show up as group policies in Security Design. You can perform all normal firewall, or NAT policy functions on these imported policies.



NOTE:

- If a group has more than 300 rules, Security Design automatically breaks the group into multiple rule groups each containing 200 rules. The only exception is that these groups are placed last in the list of groups. The size of the last group is calculated by the upper threshold of 300 rules and lower threshold of 100 rules.
- Security Design attaches \_DE to the device exception policies name. You cannot directly assign device exception policies to group policy. Assign devices to the device exception policies first, and then assign those devices to the group policies.

- Related Documentation**
- [Importing Firewall and NAT Policies from a Device to Security Design on page 207](#)

## PART 11

# Index

- [Index on page 219](#)



# Index

## A

address and address groups overview.....	31
address groups	
creating.....	38
deleting.....	39, 40
managing.....	39
modifying.....	39
addresses	
cloning.....	34
creating.....	31
deleting.....	34
duplicate objects.....	35
exporting.....	35
importing.....	35
managing.....	33
modifying.....	34
application groups	
deleting.....	29
modifying.....	29
application signatures	
creating.....	45
managing.....	47
applications	
deleting.....	26
duplicate objects.....	26
modifying.....	25

## C

conventions	
notice icons.....	xv
customer support.....	xvi
contacting JTAC.....	xvi

## D

dashboard	
overview.....	7
documentation	
comments on.....	xvi
Dynamic signature group	
creating.....	190

## E

extranet device	
cloning.....	43
managing.....	42
modifying.....	42
Extranet Device	
deleting.....	42

## F

Firewall policy	
adding rules.....	107
address book.....	87
assigning devices.....	127
cloning.....	123
cloning rules.....	125
copying or pasting rules.....	126
creating.....	90
custom column.....	119, 120, 121
See also deleting	
See also exporting	
See also managing	
See also modifying	
custom columns.....	117
See also overview	
deleting.....	122
deleting devices.....	127
deleting rules.....	125
enabling or disabling rules.....	126
exporting.....	124
grouping rules.....	125
inline object.....	98
See also creating	
modifying.....	121
multiple group policy.....	85
ordering rules.....	110
overview.....	83
priority and precedence.....	103
promoting.....	124
publishing.....	111
Firewall Policy	
custom columns.....	117
See also create	

## G

Global search.....	171
--------------------	-----

## I

IPS policy	
creating.....	195
deleting rules.....	201
enabling or disabling rules.....	201
IPS Policy	
publishing.....	198
IPS signature	
cloning.....	189
creating.....	185
deleting.....	188
filtering.....	188
modifying.....	188
IPS signature-set	
adding rules.....	192
creating.....	191
managng.....	193
IPsec VPN	
deleting.....	145
modifying.....	143
modifying endpoint settings.....	144
overview.....	131
publishing.....	141
IPsec VPNs	
creating.....	132

## M

manuals	
comments on.....	xvi

## N

NAT	
NAT policy	
publishing.....	161
NAT pool	
managing.....	53
NAT policy	
assigning devices.....	167
cloning.....	164
copying and pasting rules.....	166
creating.....	151
deleting.....	163
deleting devices.....	167
deleting rules.....	164
enabling or disabling rules.....	165
exporting.....	164
grouping rules.....	165
modifying.....	163

overview.....	149
publishing.....	161
notice icons.....	xv

## O

Object Builder overview.....	19
------------------------------	----

## S

Security design devices	
importing policies.....	207
updating.....	205
Security Design Overview.....	3
security policy profiles	
creating.....	58
managing.....	60
overview.....	57
service and service groups overview.....	21
service groups	
creating.....	27
managing.....	28
services	
creating.....	22
managing.....	25
Signature database	
downloading.....	175
installing.....	177
Static signature group	
creating.....	189
support, technical See technical support	

## T

technical support	
contacting JTAC.....	xvi

## V

VPN profiles	
creating.....	63
overview.....	63