



Junos[®] Space

Security Design User Guide

Release

11.4



Published: 2011-12-21

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
December 2011—Junos Space Security Design User Guide, Release 11.4

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	xiii
	Junos Space Documentation and Release Notes	xiii
	Documentation Conventions	xiii
	Documentation Feedback	xiv
	Requesting Technical Support	xiv
	Self-Help Online Tools and Resources	xiv
	Opening a Case with JTAC	xv
Part 1	Security Design Overview	
Chapter 1	Security Design Overview	3
	Security Design Overview	3
Chapter 2	Security Design Dashboard	7
	Security Design Dashboard	7
Part 2	Getting Started	
Chapter 3	Getting Started with Security Design	13
	Getting Started	13
	Provisioning Firewall Policies	13
	Provisioning NAT Policies	13
	Provisioning IPsec VPNs	14
	IPS Management	14
	AppFW Management	14
Part 3	Object Builder	
Chapter 4	Object Builder Overview	19
	Object Builder Overview	19
Chapter 5	Service and Service Groups	21
	Service and Service Group Overview	21
	Creating Services	22
	Managing Services	24
	Modifying a Service	24
	Deleting a Service	25
	Cloning a Service	25
	Creating Service Groups	25
	Managing Service Groups	26
	Modifying a Service Group	27
	Deleting a Service Group	27

	Cloning a Service Group	27
Chapter 6	Addresses and Address Groups	29
	Address and Address Groups Overview	29
	Creating Addresses	29
	Managing Addresses	31
	Modifying an Address	32
	Deleting an Address	32
	Cloning an Address	32
	Exporting Addresses	33
	Importing Addresses	33
	Creating Address Groups	33
	Managing Address Groups	34
	Modifying an Address Group	35
	Deleting an Address Group	35
	Cloning an Address Group	35
Chapter 7	Application Signatures	37
	Creating Application Signatures	37
	Managing Application Signatures	39
	Filtering Application Signatures	39
	Modifying Application Signatures	40
	Deleting Application Signatures	40
	Cloning Application Signatures	40
	Creating an Application Signature Group	41
Chapter 8	NAT Pools	43
	Creating NAT Pools	44
	Managing NAT Pools	45
	Deleting NAT Pools	45
	Modifying NAT Pools	46
	Cloning NAT Pools	46
Chapter 9	Policy Profiles	47
	Security Policy Profiles Overview	47
	Creating Security Policy Profiles	48
	Managing Policy Profiles	50
	Deleting Policy Profiles	51
	Modifying Policy Profiles	51
	Cloning Policy Profiles	51
Chapter 10	VPN Profiles	53
	VPN Profiles Overview	53
	Creating VPN Profiles	53
	Managing VPN Profiles	56
	Deleting VPN Profiles	56
	Modifying VPN Profiles	57
	Cloning VPN Profiles	57

Chapter 11	Variables	59
	Creating Variable Definitions	59
	Managing Variable Definitions	61
	Deleting Variable Definitions	61
	Modifying Variable Definitions	61
	Cloning Variable Definitions	62
Chapter 12	Template Definitions	63
	Creating Template Definitions	63
	Managing Template Definitions	64
	Deleting Template Definitions	64
	Modifying Template Definitions	65
Chapter 13	Templates	67
	Creating Templates	67
	Managing Templates	68
	Deleting Templates	68
	Modifying Templates	69
Part 4	Firewall Policy	
Chapter 14	Firewall Policy	73
	Firewall Policies Overview	73
	Creating Firewall Policies	74
	Adding Rules to a Firewall Policy	76
	Ordering the Rules in a Firewall Policy	79
	Publishing Firewall Policies	79
	Managing Firewall Policies	83
	Modifying Firewall Policies	84
	Deleting Firewall Policies	84
	Cloning Firewall Policies	85
	Exporting a Firewall Policy	85
	Deleting Rules in a Firewall Policy	85
	Cloning a Rule in a Firewall Policy	85
	Grouping Rules in a Firewall Policy	86
	Enabling/Disabling Rules in a Firewall Policy	86
	Assigning Devices to a Firewall Policy	87
	Deleting Devices from a Firewall Policy	87
Part 5	VPN	
Chapter 15	VPN	91
	IPsec VPN Overview	91
	Creating IPsec VPNs	92
	Publishing IPsec VPNs	96
	Managing IPsec VPNs	97
	Modifying IPsec VPNs	98
	Modifying Endpoint Settings in a VPN	99
	Deleting IPsec VPNs	99

Part 6	NAT Policies	
Chapter 16	NAT Policy	103
	NAT Overview	103
	Creating NAT Policies	104
	Adding Rules to a NAT Policy	106
	Ordering the Rules in a NAT Policy	109
	Publishing NAT Policies	110
	Managing NAT Policies	111
	Modifying NAT Policies	111
	Deleting NAT Policies	112
	Cloning NAT Policies	112
	Exporting a NAT Policy	112
	Deleting Rules in a NAT Policy	113
	Grouping Rules in a NAT Policy	113
	Enabling/Disabling Rules in a NAT Policy	113
	Assigning Devices to a NAT Policy	114
	Deleting Devices from a NAT Policy	114
Part 7	Global Search	
Chapter 17	Global Search	119
	Global Search	119
Part 8	Downloads	
Chapter 18	Downloads	123
	Downloading the Signature Database	123
	Installing the Signature Database	125
Part 9	IPS Management	
Chapter 19	IPS Management Overview	131
	IPS Management Overview	131
Chapter 20	IPS Management	133
	Creating IPS Signatures	133
	Managing IPS Signatures	135
	Filtering IPS Signatures	136
	Modifying IPS Signatures	136
	Deleting IPS Signatures	136
	Cloning IPS Signatures	137
	Creating Static Signature Groups	137
	Creating Dynamic Signature Groups	138
	Creating IPS Signature-sets	138
	Creating IPS Signature-sets	139
	Adding Rules to an IPS Signature-set	140
	Managing IPS Signature Sets	141
	Deleting IPS Signature-sets	141
	Cloning IPS Signature-sets	141

	Enable or Disable Rules in an IPS Signature-set	142
	Creating IPS Policies	143
	Managing IPS Policies	144
	Deleting IPS Policy Rules	144
	Enabling or Disabling Rules in an IPS Policy	144
Part 10	Security Design Devices	
Chapter 21	Security Design Devices	149
	Updating Devices with Pending Services	149
Part 11	Index	
	Index	153

List of Figures

Part 1	Security Design Overview	
Chapter 1	Security Design Overview	3
	Figure 1: Security Design Home Page	4
Chapter 2	Security Design Dashboard	7
	Figure 2: Object Count Gadget	9
	Figure 3: Address Types Gadgets	9
Part 3	Object Builder	
Chapter 5	Service and Service Groups	21
	Figure 4: Create Service Page	22
	Figure 5: Create Service Group Page	26
Chapter 6	Addresses and Address Groups	29
	Figure 6: Create Address Page	30
	Figure 7: Create Address Group Page	34
Chapter 7	Application Signatures	37
	Figure 8: Application Signatures Page	37
	Figure 9: Create Application Signature Page	38
Chapter 8	NAT Pools	43
	Figure 10: Create NAT Pool Page	44
Chapter 9	Policy Profiles	47
	Figure 11: New Policy Profile Page	49
Chapter 10	VPN Profiles	53
	Figure 12: VPN Profile: Phase 1	54
	Figure 13: VPN Profile: Phase 2	55
Chapter 11	Variables	59
	Figure 14: Create Polymorphic Address Page	60
Chapter 12	Template Definitions	63
	Figure 15: Create Template Definition Page	64
Chapter 13	Templates	67
	Figure 16: Create Template Page	68
Part 4	Firewall Policy	
Chapter 14	Firewall Policy	73

	Figure 17: Firewall Policy Tabular View	74
	Figure 18: Create Firewall Policy Page	75
	Figure 19: Selecting Policies to Publish	80
	Figure 20: Devices on Which the Policies Will be Published	81
	Figure 21: Policy Publish: CLI Configuration	81
	Figure 22: Policy Publish: XML Configuration	82
Part 5	VPN	
Chapter 15	VPN	91
	Figure 23: VPN Tabular View	92
	Figure 24: Create VPN Page 1	93
	Figure 25: Create VPN Page 2	94
	Figure 26: Create VPN Page 3	95
	Figure 27: VPN Preview	96
Part 6	NAT Policies	
Chapter 16	NAT Policy	103
	Figure 28: NAT Policy Tabular View	104
	Figure 29: Create NAT Policy Page	105
Part 7	Global Search	
Chapter 17	Global Search	119
	Figure 30: Global Search Results	119
Part 8	Downloads	
Chapter 18	Downloads	123
	Figure 31: Signature Download Logs	123
	Figure 32: Signature Database Page	124
	Figure 33: Download Configuration Page	124
	Figure 34: Install Configuration Page	126
Part 9	IPS Management	
Chapter 20	IPS Management	133
	Figure 35: View All IPS Signatures Page	134
	Figure 36: Create IPS Signature Page	134
	Figure 37: IPS Signature Set Tabular View	139
	Figure 38: IPS Policies Tabular View	143
Part 10	Security Design Devices	
Chapter 21	Security Design Devices	149
	Figure 39: Security Design Devices Page	149
	Figure 40: Update Window	150

List of Tables

	About This Guide	xiii
	Table 1: Notice Icons	xiii
Part 1	Security Design Overview	
Chapter 2	Security Design Dashboard	7
	Table 2: Security Design Workspaces	8
Part 4	Firewall Policy	
Chapter 14	Firewall Policy	73
	Table 3: IPS Field Options	78
Part 7	Global Search	
Chapter 17	Global Search	119
	Table 4: Security Design Global Search	119

About This Guide

- Junos Space Documentation and Release Notes on page xiii
- Documentation Conventions on page xiii
- Documentation Feedback on page xiv
- Requesting Technical Support on page xiv

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 xiii 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, 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.

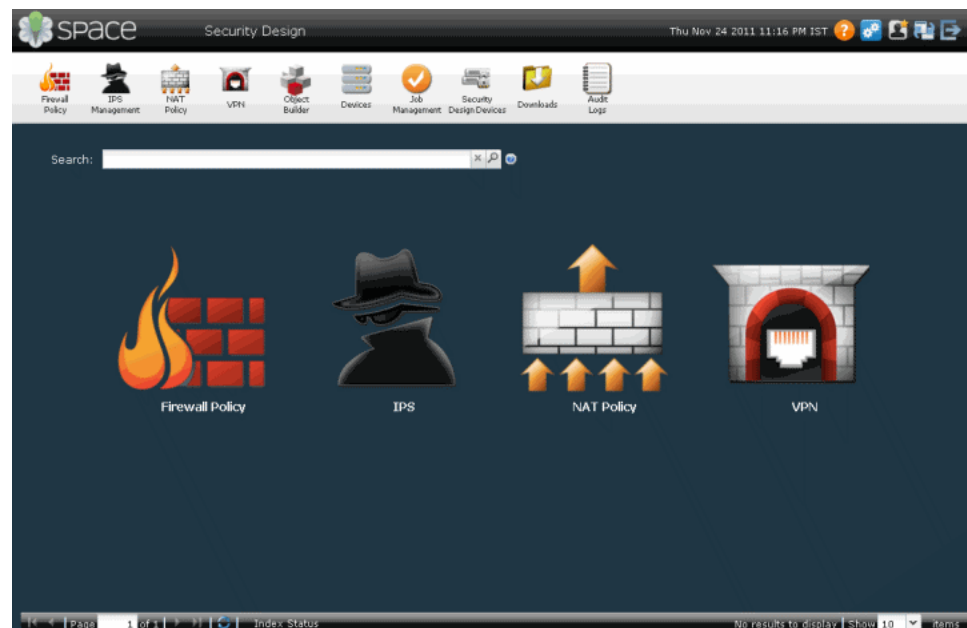
A set of gadgets displayed on the dashboard graphically illustrates the critical elements related to your security configurations. These gadgets help you keep track of the objects created and their usage across security configurations.

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

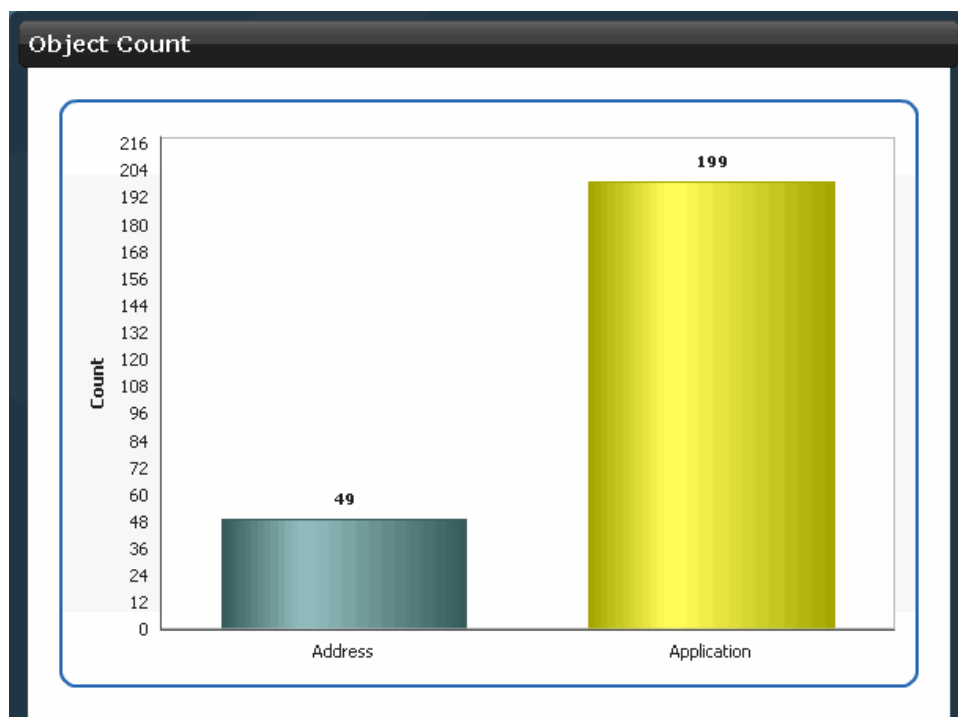
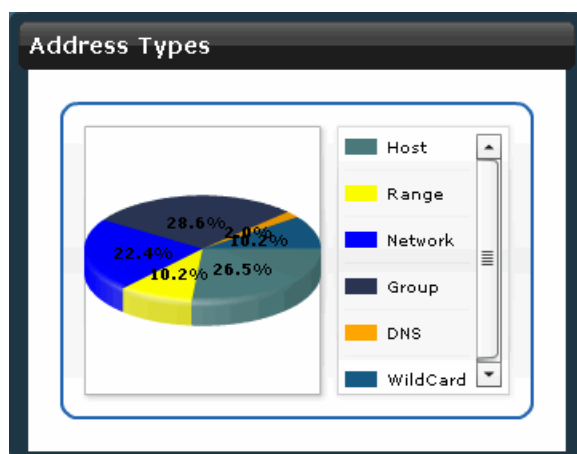


Figure 3 on page 9 shows the Address Types gadget. This gadget shows the different address types created using the Address Creation Wizard.

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 29](#).
3. Create a policy profile. See [“Creating Policy Profiles” on page 48](#).
4. Create a service. See [“Creating Services” on page 22](#).
5. Create firewall policies. See [“Creating Firewall Policies” on page 74](#).
6. Publish firewall policies. See [“Publishing Firewall Policies” on page 79](#)
7. Update devices. See [“Updating Devices with Pending Services” on page 149](#).

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 29](#).
3. Create firewall policies. See [“Creating Firewall Policies” on page 74](#).
4. Publish firewall policies. See [“Publishing Firewall Policies” on page 79](#)
5. Create NAT pools. See [“Creating NAT Pools” on page 44](#)
6. Create NAT policies. See [“Creating NAT Policies” on page 104](#).
7. Publishing NAT policies. See [“Publishing NAT Policies” on page 110](#)
8. Update devices. See [“Updating Devices with Pending Services” on page 149](#).

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 29](#).
3. Create a VPN profile. See [“Creating VPN Profiles” on page 53](#).
4. Create an IPsec VPN. See [“Creating IPsec VPNs” on page 92](#).
5. Publish the IPsec VPN. See [“Publishing IPsec VPNs” on page 96](#).
6. Update devices. See [“Updating Devices with Pending Services” on page 149](#).

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 123](#).
3. Pushing IPS signature to the device. See [“Installing the Signature Database” on page 125](#).
4. Create a firewall policy with IPS enabled. See [“Creating Firewall Policies” on page 74](#).
5. Publish firewall policies. See [“Publishing Firewall Policies” on page 79](#).
6. Update devices. See [“Updating Devices with Pending Services” on page 149](#).
7. Create IPS signature. See [“Creating IPS Signatures” on page 133](#).
8. Create IPS signature-set. See [“Creating IPS Signature Sets” on page 139](#).
9. Create IPS policies. See [“Creating IPS Policies” on page 143](#).

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 123](#).
3. Push application signature to the device. See [“Installing the Signature Database” on page 125](#).
4. Create a firewall policy with AppFW enabled. See [“Creating Firewall Policies” on page 74](#).
5. Publish firewall policies. See [“Publishing Firewall Policies” on page 79](#).
6. Update devices. See [“Updating Devices with Pending Services” on page 149](#).
7. Create application signature. See [“Creating Application Signatures” on page 37](#).

PART 3

Object Builder

- [Object Builder Overview on page 19](#)
- [Service and Service Groups on page 21](#)
- [Addresses and Address Groups on page 29](#)
- [Application Signatures on page 37](#)
- [NAT Pools on page 43](#)
- [Policy Profiles on page 47](#)
- [VPN Profiles on page 53](#)
- [Variables on page 59](#)
- [Template Definitions on page 63](#)
- [Templates on page 67](#)

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
- 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 29](#)
- [Service and Service Groups Overview on page 21](#)
- [Policy Profiles Overview on page 47](#)
- [VPN Profiles Overview on page 53](#)

CHAPTER 5

Service and Service Groups

- [Service and Service Group Overview on page 21](#)
- [Creating Services on page 22](#)
- [Managing Services on page 24](#)
- [Creating Service Groups on page 25](#)
- [Managing Service Groups on page 26](#)

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

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 25](#)
- [Managing Services on page 24](#)
- [Managing Service Groups on page 26](#)

Creating Services

To create a service:

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

The **Manage Services** page appears with all the services.

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

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

Figure 4: Create Service Page

Create Service

Name:

Description:

Protocols: + ✎ ✖

Name	Type	Detail
TCP	TCP	ALG:None Source Port: 0-65535 Destination Port: 0-65535 Inactivity Timeout: Never
UDP	UDP	ALG:None Source Port: 0-65535 Destination Port: 0-65535 Inactivity Timeout: Never

3. Enter the name of the service in the **Name** field.
4. Enter the description for the service in the **Description** field.
5. In the **Protocols** pane, click the **Add** icon to add a new protocol.
The **New Protocol** dialog box appears with default values.
6. Enter a name for the new protocol in the **Name** section.
7. Click the **Enable Inactivity Timeout** check box if you want to enable this option.
8. Enter a value in seconds in the **Inactivity Timeout** field.

The default value is 300 seconds.

9. Select a protocol type from the **Type** drop-down menu.

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

- TCP
 - a. Select the appropriate option from the **ALG** drop-down menu.
 - b. Enter a range of TCP source ports in the **Source Port** field.
 - c. Enter a range of TCP destination ports in the **Destination Port** field.
- UDP
 - a. Select the appropriate option from the **ALG** drop-down menu.
 - b. Enter a range of TCP source ports in the **Source Port** field.
 - c. Enter a range of TCP destination ports in the **Destination Port** field.
- ICMP
 - a. Enter a value pertaining to the ICMP message you want to display in the **ICMP Type** field.
 - b. Enter a value associated with the ICMP type you have specified in the **ICMP Code** field.
- SUN - RPC
 - a. Enter a value corresponding to 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.
- Other
 - a. Select the appropriate option from the **ALG** drop-down menu.
 - b. Enter a range of TCP source ports in the **Source Port** field.
 - c. Enter a range of TCP destination ports in the **Destination Port** field.
 - d. Enter the protocol 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.

10. Click **Add** in the **New Protocol** dialog box.
11. Click **Create** to create a service.

**Related
Documentation**

- [Service and Service Groups Overview on page 21](#)
- [Creating Service Groups on page 25](#)
- [Managing Services on page 24](#)
- [Managing Service Groups on page 26](#)

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 24](#)
2. [Deleting a Service on page 25](#)
3. [Cloning a Service on page 25](#)

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**.

Related Documentation

- [Service and Service Groups Overview on page 21](#)
- [Creating Services on page 22](#)
- [Creating Service Groups on page 25](#)
- [Managing Service Groups on page 26](#)

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 5 on page 26](#).

Figure 5: Create Service Group Page

The screenshot shows the 'Create Service Group' interface. The 'Name' field contains 'New_App_Group'. The 'Description' field is empty. The 'Members' section has an 'Add' icon. A 'Select Services' dialog box is open, displaying two panes: 'Available' and 'Selected'. The 'Available' pane lists services: aol, apple-ichat-snatmap, bgp, bootps, chargen, and cvspserver. The 'Selected' pane lists: apple-ichat, biff, bootpc, and cifs. There are 'Select' and 'Cancel' buttons at the bottom of the dialog.

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 Groups Overview on page 21](#)
- [Managing Service Groups on page 26](#)
- [Creating Services on page 22](#)
- [Managing Services on page 24](#)

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 27](#)
2. [Deleting a Service Group on page 27](#)
3. [Cloning a Service Group on page 27](#)

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 Groups Overview on page 21](#)
- [Creating Service Groups on page 25](#)
- [Creating Services on page 22](#)
- [Managing Services on page 24](#)

CHAPTER 6

Addresses and Address Groups

- [Address and Address Groups Overview on page 29](#)
- [Creating Addresses on page 29](#)
- [Managing Addresses on page 31](#)
- [Creating Address Groups on page 33](#)
- [Managing Address Groups on page 34](#)

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 29](#)
- [Managing Addresses on page 31](#)
- [Creating Address Groups on page 33](#)
- [Managing Address Groups on page 34](#)

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 6 on page 30](#).

Figure 6: 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 29](#)
- [Managing Addresses on page 31](#)
- [Creating Address Groups on page 33](#)
- [Managing Address Groups on page 34](#)

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 32](#)
2. [Deleting an Address on page 32](#)
3. [Cloning an Address on page 32](#)
4. [Exporting Addresses on page 33](#)
5. [Importing Addresses on page 33](#)

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**.

Related Documentation

- [Address and Address Groups Overview on page 29](#)
- [Creating Addresses on page 29](#)
- [Creating Address Groups on page 33](#)
- [Managing Address Groups on page 34](#)

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 7 on page 34](#).

Figure 7: Create Address Group Page

Create Address Group

Name:

Description:

Addresses: 

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 29](#)
 - [Managing Address Groups on page 34](#)
 - [Creating Addresses on page 29](#)
 - [Managing Addresses on page 31](#)

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 35](#)
2. [Deleting an Address Group on page 35](#)
3. [Cloning an Address Group on page 35](#)

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 29](#)
- [Creating Address Groups on page 33](#)
- [Creating Addresses on page 29](#)
- [Managing Addresses on page 31](#)

CHAPTER 7

Application Signatures

- Creating Application Signatures on page 37
- Managing Application Signatures on page 39

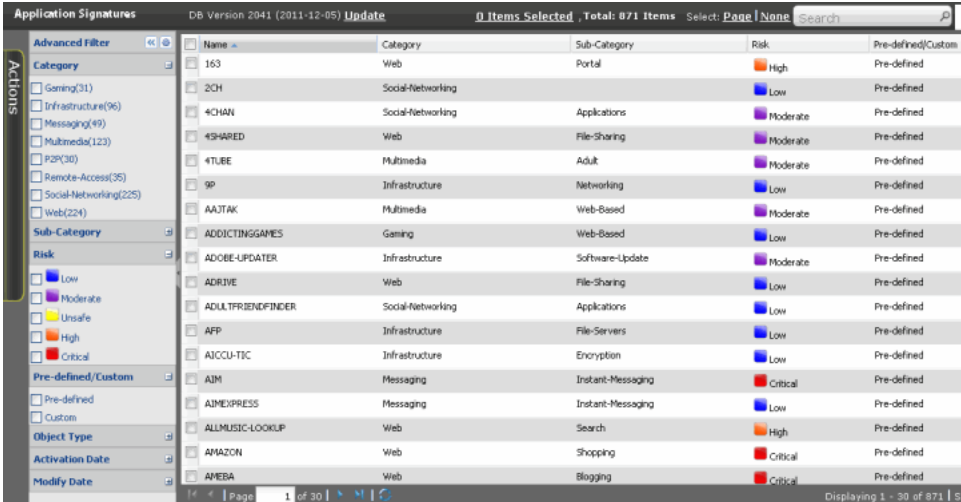
Creating Application Signatures

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 8 on page 37](#). 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 8: 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
ADRIVE	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
AJM	Messaging	Instant-Messaging	Critical	Pre-defined
AJMESPRESS	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 9 on page 38](#).



Figure 9: 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:

- 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 39](#)

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 39](#)
- [Modifying Application Signatures on page 40](#)
- [Deleting Application Signatures on page 40](#)
- [Cloning Application Signatures on page 40](#)
- [Creating an Application Signature Group on page 41](#)

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 8

NAT Pools

- [Creating NAT Pools on page 44](#)
- [Managing NAT Pools on page 45](#)

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 10 on page 44](#).

Figure 10: Create NAT Pool Page

The screenshot shows the 'Create NAT Pool' dialog box. The 'Name' field is filled with 'Pool_1'. The 'Description' field is empty. The 'Pool Type' dropdown is set to 'SOURCE'. The 'Pool Address' dropdown is set to 'AccountsDept'. The 'Advanced' section is expanded, showing 'Host Address Base' as an empty field, 'Translation' set to 'No Translation', and 'Overflow Pool Type' set to 'None'. The 'Create' and 'Cancel' buttons are at the bottom.

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** drop-down menu.
5. Select the appropriate address from the **Pool Address** drop-down menu.
6. Expand the **Advanced** pane by clicking the down arrow.
7. Enter an appropriate value in the **Host Address Base** field.
8. Select the appropriate option from the **Translation** drop-down menu.
 - If you select **Port/Range** in the **Translation** drop-down menu, a new field named **Port** appears.
 - Select an appropriate option from the **Port** drop-down menu.

- If you select **Overload** in the **Translation** drop-down menu, a new option named **Port Overloading Factor** appears.
 - Select an appropriate value from the **Port Overloading Factor** selector.
9. Select the appropriate option from the **Overflow Pool Type** drop-down menu.
 - If you select **Pool** in the **Overflow Pool Type** drop-down menu, a new field named **Overflow Pool** appears.
 - Select the appropriate NAT pool from the **Overflow Pool** selector.
 10. Click **Create**.

**Related
Documentation**

- [NAT Overview on page 103](#)
- [Managing NAT Pools on page 45](#)
- [Creating NAT Policies on page 104](#)
- [Managing NAT Policies on page 111](#)

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 45](#)
- [Modifying NAT Pools on page 46](#)
- [Cloning NAT Pools on page 46](#)

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 103](#)
- [Creating NAT Pools on page 44](#)
- [Creating NAT Policies on page 104](#)
- [Managing NAT Policies on page 111](#)

CHAPTER 9

Policy Profiles

- [Security Policy Profiles Overview on page 47](#)
- [Creating Security Policy Profiles on page 48](#)
- [Managing Policy Profiles on page 50](#)

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 48](#)
- [Managing Policy Profiles on page 50](#)

Creating Security 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 11 on page 49](#).

Figure 11: 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**
- [Policy Profiles Overview on page 47](#)
 - [Managing Policy Profiles on page 50](#)

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 51](#)
- [Modifying Policy Profiles on page 51](#)
- [Cloning Policy Profiles on page 51](#)

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 10

VPN Profiles

- [VPN Profiles Overview on page 53](#)
- [Creating VPN Profiles on page 53](#)
- [Managing VPN Profiles on page 56](#)

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 53](#)
- [Managing VPN Profiles on page 56](#)

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 12 on page 54](#) shows the Phase 1 tab.

Figure 12: VPN Profile: Phase 1

The screenshot shows the 'VPN Profile' configuration window with the 'Phase 1' tab selected. The 'Name' field is 'Bng_IT' and the 'Description' field is empty. Under 'Mode', 'Aggressive' is selected. The 'IKE Id' dropdown is set to 'Hostname'. 'Authentication Type' is 'Preshared Key'. Under 'Proposals', 'Predefined' is selected, with 'Basic' chosen from the sub-options. The '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. 'Create' and 'Cancel' buttons are at the bottom.

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 13 on page 55 shows the Phase 2 tab.

Figure 13: 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 like 'Establish tunnel immediately', 'Enable VPN Monitor', 'DF bit' (set to 'None'), 'Idle time(secs)' (set to 60), 'Install time' (set to 1), and 'Enable Anti Replay'. '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 53](#)
 - [Managing VPN Profiles on page 56](#)

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 56](#)
- [Modifying VPN Profiles on page 57](#)
- [Cloning VPN Profiles on page 57](#)

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 11

Variables

- [Creating Variable Definitions on page 59](#)
- [Managing Variable Definitions on page 61](#)

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 Address** page appears, as shown in [Figure 14 on page 60](#). You can create a variable definition on this page.

Figure 14: Create Polymorphic Address Page

Create Polymorphic Address

Name:

Description:

Default Address:

Type:

<input type="checkbox"/>	Context Value	Variable Value
<input checked="" type="checkbox"/>	10.205.230.9	64.74.223.36/32
<input type="checkbox"/>	10.205.230.5	64.58.240.32/27

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 from the **Type** drop-down menu.
6. Enter a value in the **Default Address** field.
7. To add variable values:
 - a. Click the Add icon.
A new row appears.
 - b. Double-click **Context Value** field and select the device.
 - c. Double-click **Variable Value** field and enter the variable value.
8. Click **Create**.

Related Documentation

- [Managing Variable Definitions on page 61](#)

Managing Variable Definitions

You can delete, modify, or clone, variable definitions listed in 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 61](#)
- [Modifying Variable Definitions on page 61](#)
- [Cloning Variable Definitions on page 62](#)

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**.

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 63](#)
- [Managing Template Definitions on page 64](#)

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**.

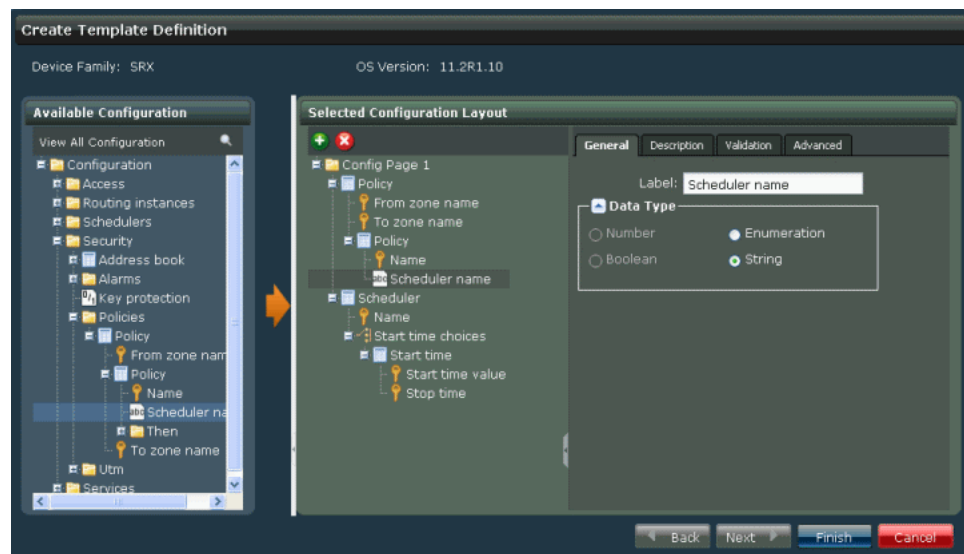
The **Create Template Definition** page appears.

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 15 on page 64](#).

Figure 15: Create Template Definition Page



9. Click **Finish**.

The new template definition is created.

Related Documentation

- [Managing Template Definitions on page 64](#)

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 64](#)
- [Modifying Template Definitions on page 65](#)

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

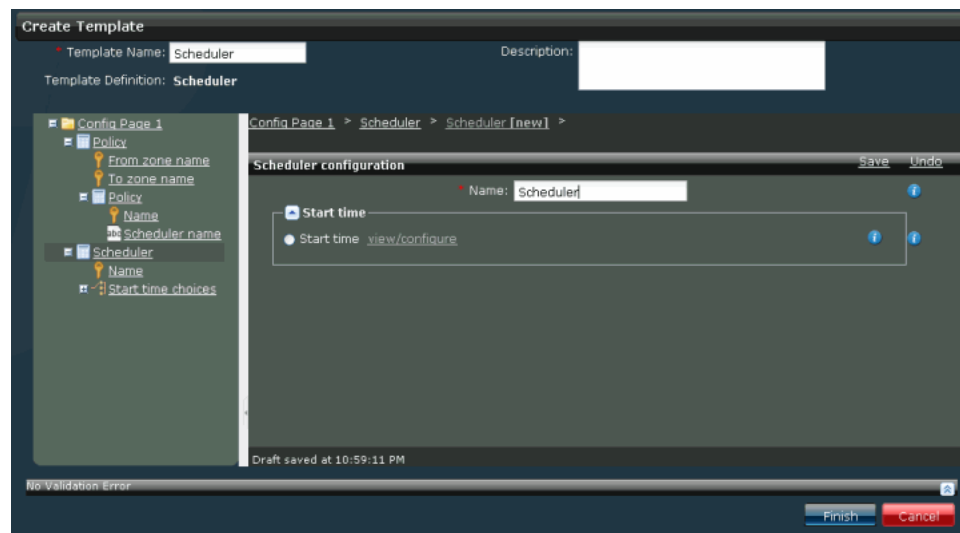
- [Creating Templates on page 67](#)
- [Managing Templates on page 68](#)

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 16 on page 68](#).

Figure 16: Create Template Page



9. Click **Finish**.

Related Documentation

- [Managing Templates on page 68](#)

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 68](#)
- [Modifying Templates on page 69](#)

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 73](#)

CHAPTER 14

Firewall Policy

- [Firewall Policies Overview on page 73](#)
- [Creating Firewall Policies on page 74](#)
- [Adding Rules to a Firewall Policy on page 76](#)
- [Ordering the Rules in a Firewall Policy on page 79](#)
- [Publishing Firewall Policies on page 79](#)
- [Managing Firewall Policies on page 83](#)

Firewall Policies Overview

Security Design provides you with four types of firewall policies which include:

- **Global Policy:** Global policy is predefined firewall policy that is available with Security Design. You can add pre rules, and post rules. When the global policy configuration is updated on the devices, the rules are updated in the following order - global pre rules, group pre rules, device-specific rules, group post rules, and global post rules.
- **Group Policy:** Group policy is a 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 pre rules, group post rules, and device rules for a group policy. When a group firewall policy is updates on the devices, the rules are updated in the following order - group pre rules, device-specific rules, and group post rules.
- **Device Policy:** Device policy is a 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
- **Device-exception Policy:** Device-exception policy is created when a device is removed from a group policy.

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.

Related Documentation

- [Creating Firewall Policies on page 74](#)
- [Adding Rules to a Firewall Policy on page 76](#)
- [Ordering the Rules in a Firewall Policy on page 79](#)
- [Managing Firewall Policies on page 83](#)
- [Publishing Firewall Policies on page 79](#)

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 17 on page 74](#).

Figure 17: Firewall Policy Tabular View

S.No.	Name	Source Zone	Source Address	Destination Zone	Destination Address	Service	Action	AppFW	Profile	IPS	Description
Global Policy Pre Rules (1 rule)											
Corporate-Policy-Main Pre Rules (3 rules)											
1	Corporate-2-Branch1-1	trust	Corp-Desktop-Users	untrust	Branch1-Users	Rtp, Http, Http-ext, ssh	Permit + SPI	-	All Logging Enabled	Web_Server	Corporate to bra
2	Mobile-VPN-Users	trust	Mobile-VPN	untrust	VPN-SERVER	Https	Permit + SPI	-	All Logging Disabled	File_Server	VPN Users to VPN
3	Corp-DHCP-DNS	trust	Corp-DNS-DHCP	untrust	grutella, telnet		Reject	-	LOG		Corporate DNS at
Corporate-Policy-Main Post Rules (4 rules)											
1	Corp-2-Branch1-1	trust	Corp-Desktop-Users	untrust	Group-Rail-1	Rtp, Rtp-get, Http, Https	Permit + SPI	-	LOG		DNS_Services Corporate to bra
2	Corp-DNS2	trust	ALL-WEB_GROUP, Corp-DNS2	untrust	Partner-NW	Http	Permit + SPI	-	AUTHPT		DNS_Services DNS2 Access
3	Corp-DNS2-2	trust	DHCP, Corp-DNS2	untrust	Partner-NW	Http, Https	Permit + SPI	-	AUTH_WEB		DNS_Services DNS2 Access
4	Deny-All	trust	Any	untrust	Any	Any	Deny	-			Default Deny all
Global Policy Post Rules (1 rule)											

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

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 in the **Description** field.
 - c. Select the profile for the group policy from the **Profile** drop-down menu.
 - d. Select the IPS mode from the **IPS Configuration Mode** drop-down menu.

- e. Click the **Show Assigned Devices** check box to make the devices on which policies have been configured available for selection.
- f. 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 18 on page 75](#).

Figure 18: Create Firewall Policy Page

- g. 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** drop-down menu.
 - d. Select the IPS mode from the **IPS Configuration Mode** drop-down menu.

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



NOTE: When you are viewing a group policy, if you do not want the global 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.

Related Documentation

- [Firewall Policies Overview on page 73](#)
- [Adding Rules to a Firewall Policy on page 76](#)
- [Ordering the Rules in a Firewall Policy on page 79](#)
- [Managing Firewall Policies on page 83](#)
- [Publishing Firewall Policies on page 79](#)

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.

14. Click **OK**.

15. 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.

18. Click **OK**.

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

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

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 3 on page 78](#) displays the options available based on the **IPS Configuration Mode**.

Table 3: 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, Express, 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, you will see a confirmation window to save the changes you have made.

Related Documentation

- [Firewall Policies Overview on page 73](#)
- [Creating Firewall Policies on page 74](#)
- [Ordering the Rules in a Firewall Policy on page 79](#)
- [Managing Firewall Policies on page 83](#)
- [Publishing Firewall Policies on page 79](#)

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.
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 73](#)
- [Creating Firewall Policies on page 74](#)
- [Adding Rules to a Firewall Policy on page 76](#)
- [Managing Firewall Policies on page 83](#)
- [Publishing Firewall Policies on page 79](#)

Publishing Firewall Policies

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.

- Click the **Schedule at a later time** check box if you want to schedule and publish the configuration later as shown in [Figure 19 on page 80](#).

Figure 19: Selecting Policies to Publish

Name	Publish State
Global Policy	Not Published
Corporate-Policy-Main	Published
10.205.119.108	Not Published

☒ **Schedule at a later time**

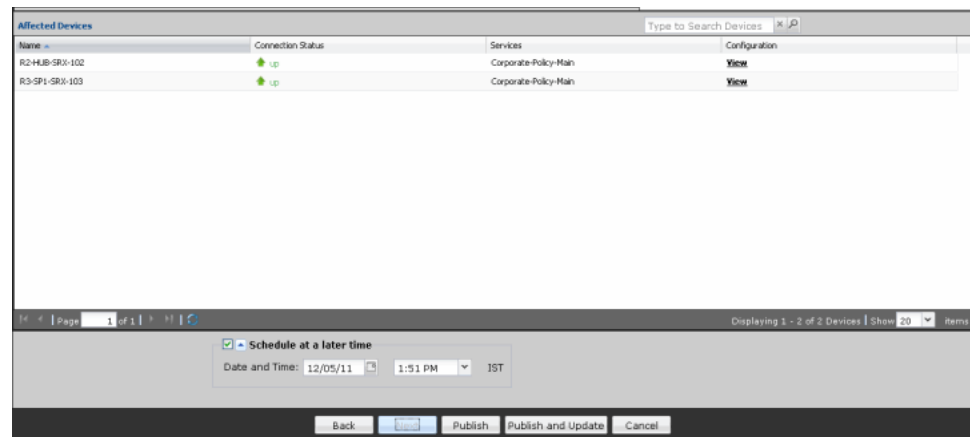
Date and Time: 12/05/11 1:51 PM IST

Back Next Publish Publish and Update Cancel

- Click **Next**.

The **Affected Devices** page displays the devices on which the policies will be published as shown in [Figure 20 on page 81](#).

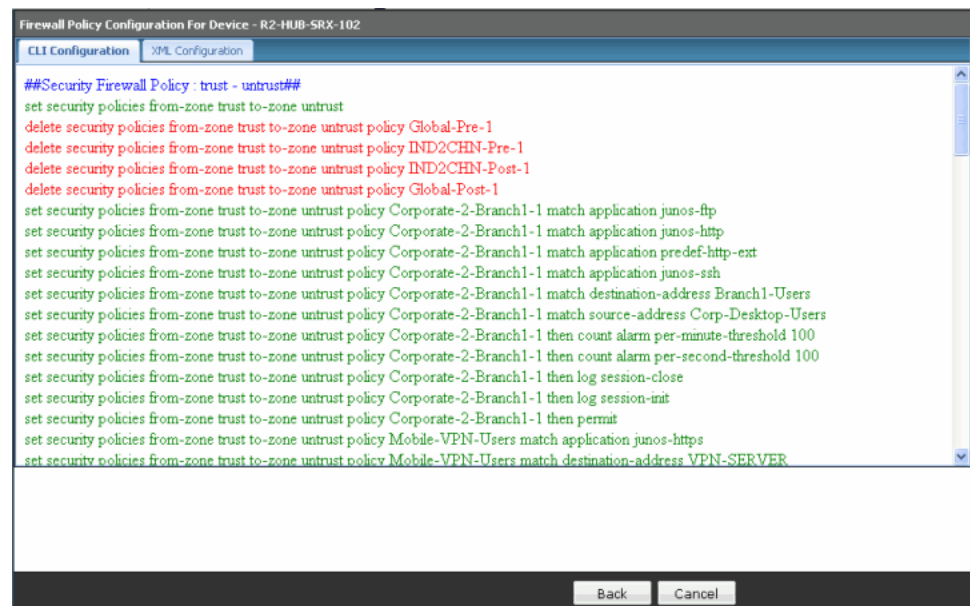
Figure 20: Devices on Which the Policies Will be Published



- 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 21 on page 81.

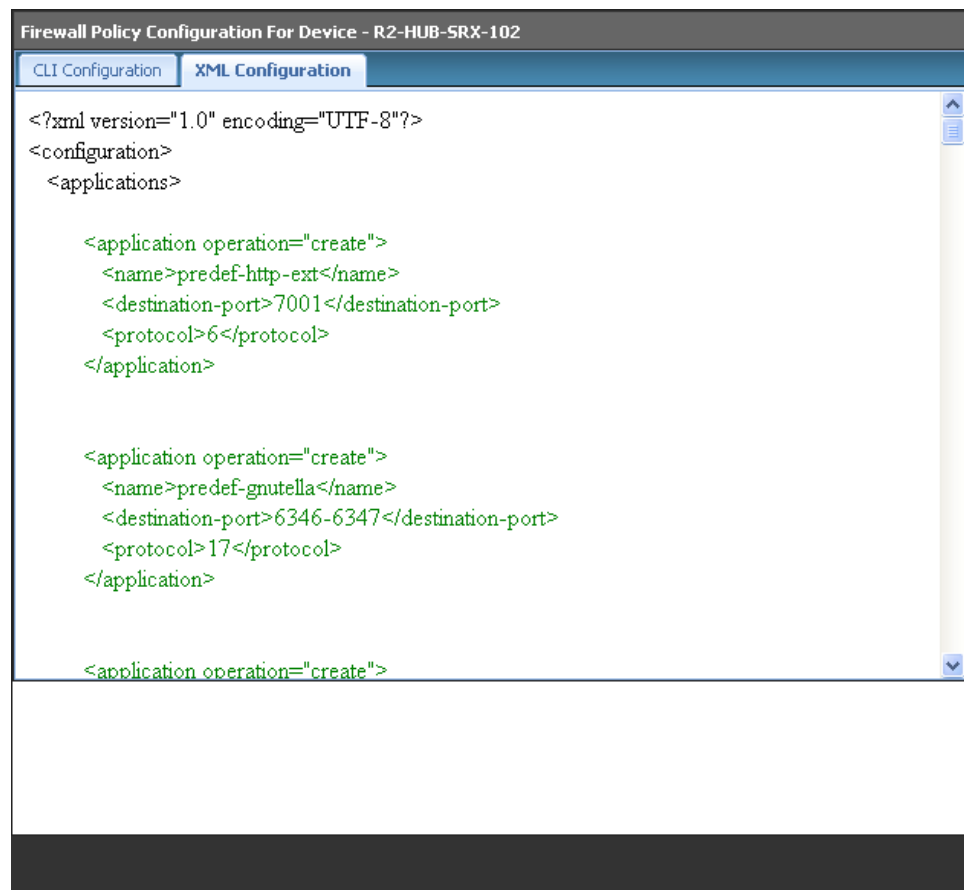
Figure 21: Policy Publish: CLI Configuration



NOTE: You cannot view the CLI configuration if you have used custom objects in the firewall policy.

- View the XML format of the configuration by clicking the **XML Configuration** tab as shown in Figure 22 on page 82.

Figure 22: Policy Publish: XML Configuration



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 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.

10. 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 global policy.



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 73](#)
- [Creating Firewall Policies on page 74](#)
- [Adding Rules to a Firewall Policy on page 76](#)
- [Ordering the Rules in a Firewall Policy on page 79](#)
- [Managing Firewall Policies on page 83](#)

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 84](#)
2. [Deleting Firewall Policies on page 84](#)
3. [Cloning Firewall Policies on page 85](#)
4. [Exporting a Firewall Policy on page 85](#)
5. [Deleting Rules in a Firewall Policy on page 85](#)
6. [Cloning a Rule in a Firewall Policy on page 85](#)
7. [Grouping Rules in a Firewall Policy on page 86](#)
8. [Enabling/Disabling Rules in a Firewall Policy on page 86](#)
9. [Assigning Devices to a Firewall Policy on page 87](#)
10. [Deleting Devices from a Firewall Policy on page 87](#)

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.

3. 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.

.....

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, and IPS mode of the firewall policy.

3. Click **Clone**.

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.

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 73](#)
- [Creating Firewall Policies on page 74](#)
- [Adding Rules to a Firewall Policy on page 76](#)
- [Ordering the Rules in a Firewall Policy on page 79](#)
- [Publishing Firewall Policies on page 79](#)

PART 5

VPN

- [VPN on page 91](#)

CHAPTER 15

VPN

- [IPsec VPN Overview on page 91](#)
- [Creating IPsec VPNs on page 92](#)
- [Publishing IPsec VPNs on page 96](#)
- [Managing IPsec VPNs on page 97](#)

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 at a per tunnel.

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

Related Documentation

- [Creating IPsec VPNs on page 92](#)
- [Managing IPsec VPNs on page 97](#)
- [Publishing IPsec VPNs on page 96](#)

Creating IPsec VPNs

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

The VPN Tabular view appears, as shown in [Figure 23 on page 92](#).

Figure 23: VPN Tabular View

Device	External Interface	Tunnel Zone	Protected Zone/Networks
10.205.61.38	ge-0/0/2.0 (10.205.61.38)	DMZ0	Addresses AccountsDept
R2-HUB-SRX-102	ge-0/0/1.0 (11.11.11.2)	untrust	Addresses ALL-WEB_GROUP
SRX210B-119-105-EP2	fe-0/0/3.0	trust	Addresses Branch1-Users

2. From the task ribbon, select the **Create VPN** icon.
- The **Create VPN** window 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 option button next to the type of VPN you want to create.
 6. Select the VPN profile from the **VPN Profile** drop-down menu.



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

7. Select the option button next to the type of preshared key.
 - a. 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 24 on page 93](#).

Figure 24: Create VPN Page 1

Create VPN

Name:

Description:

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

VPN Profile:

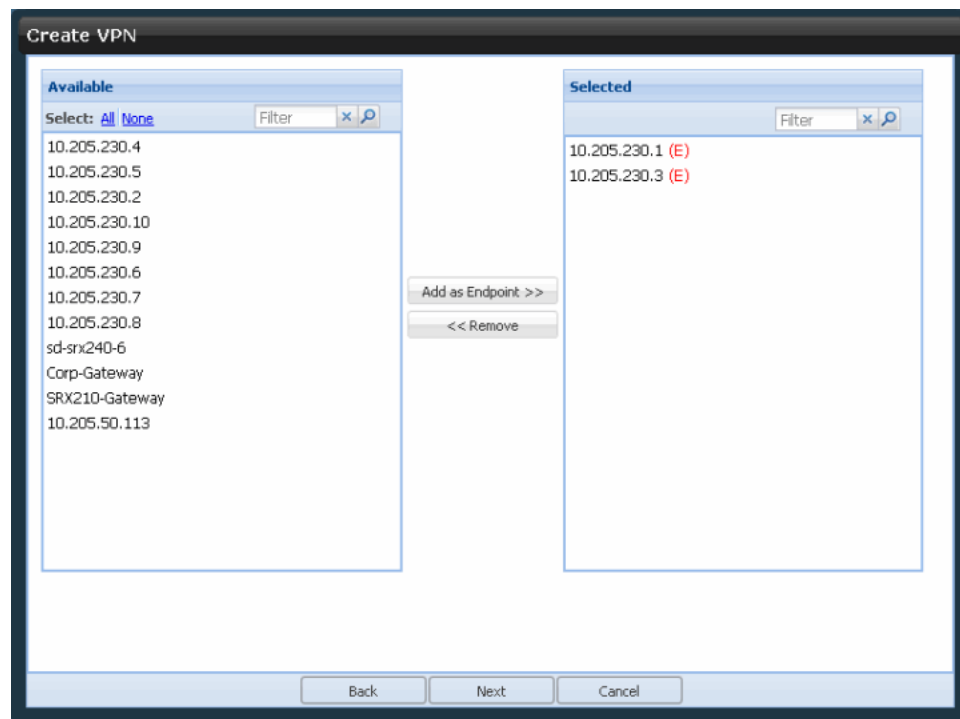
Preshared Key: ☒ Auto-generate ☐ Manual

☒ Generate Unique key per tunnel

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

This page displays the **Available** and **Selected** pane.
9. Select the device from the **Available** column and click **Add as Endpoint** as shown in [Figure 25 on page 94](#).

Figure 25: Create VPN Page 2



The device is moved to the **Selected** section.



NOTE: You will see the **Add as Hub** button if you have chosen to create a hub-and-spoke VPN type.

10. Click **Next**.

11. Select the type of interface 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** as the peers-per-tunnel-interface, enter the values in the **Specify Values** field as shown in [Figure 26 on page 95](#).

Figure 26: Create VPN Page 3

Create VPN

Tunnel Settings

Interface Type: ☐ Unnumbered ☒ Numbered

IP Subnet:

No. of Peer devices per tunnel interface: ☒ All ☐ Specify Values

Route Settings

Routing Options: ☒ Static Routing ☐ No Routing

Global Settings

Endpoint Configurations

External Interface:

Tunnel Zone:

Protected Network Zone:

Back Next Cancel

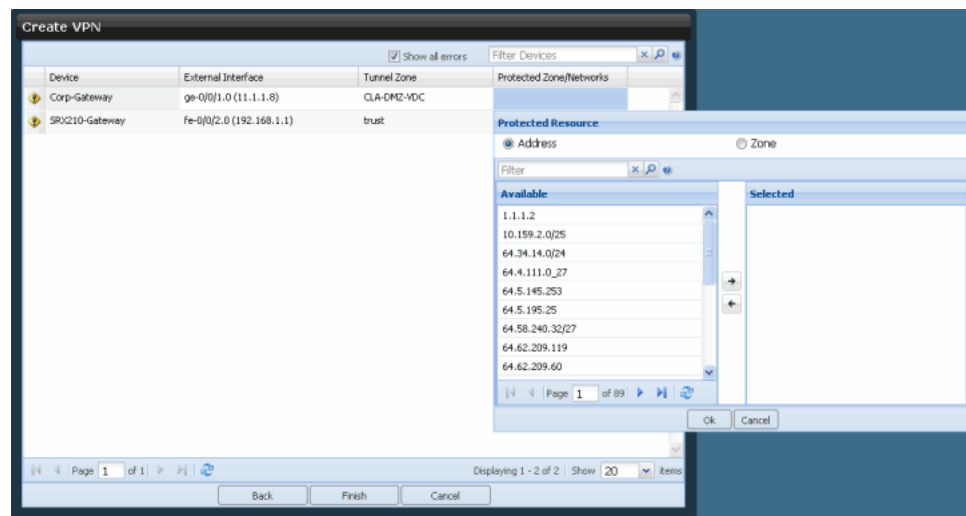
12. Select the routing option in the **Routing options** pane.
13. In the **Global Settings** pane, under **Endpoint Configurations**, enter the external interface in the **External Interface** field.
14. In the **Global Settings** pane, under **Endpoint Configurations**, enter the tunnel zone in the **Tunnel Zone** field.
15. In the **Global Settings** pane, under **Endpoint Configurations**, enter the zone type in the **Protected Network Zone** field.

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

16. If you have select Static routing, enter the external interface in the **External Interface** field under **Endpoint Configurations**.
17. If you have select Static routing, enter the tunnel zone in the **Tunnel Zone** field under **Endpoint Configuration**.
18. Click **Next**.

This page shows the preview of the values entered for the VPN, as shown in [Figure 27 on page 96](#). This page gives 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 the errors in the configuration. You would need to modify the configuration to eliminate any errors and then proceed to the next step.

Figure 27: VPN Preview



19. Click **Finish**.

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 91](#)
- [Creating IPsec VPNs on page 92](#)
- [Managing IPsec VPNs on page 97](#)

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 98](#)
2. [Modifying Endpoint Settings in a VPN on page 99](#)
3. [Deleting IPsec VPNs on page 99](#)

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. 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 91](#)
- [Creating IPsec VPNs on page 92](#)
- [Publishing IPsec VPNs on page 96](#)

PART 6

NAT Policies

- [NAT Policy on page 103](#)

CHAPTER 16

NAT Policy

- [NAT Overview on page 103](#)
- [Creating NAT Policies on page 104](#)
- [Adding Rules to a NAT Policy on page 106](#)
- [Ordering the Rules in a NAT Policy on page 109](#)
- [Publishing NAT Policies on page 110](#)
- [Managing NAT Policies on page 111](#)

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 local area network. An untrust zone is the Internet. NAT modifies the IP addresses of the packets moving between the trust and untrust zones.

Whenever a packet comes to 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.

Related Documentation

- [Creating NAT Policies on page 104](#)
- [Publishing NAT Policies on page 110](#)
- [Managing NAT Policies on page 111](#)
- [Managing NAT Pools on page 45](#)

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 28 on page 104](#). 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 28: NAT Policy Tabular View

NAT

Filter

Corp-Gateway

Filter Rules

Show Guard Policy

S.No.	Name	NAT Type	Original Packet Source		Original Packet Destination			Translated Packet Source	Translated Packet Destination	Description
			Ingress	Address	Egress	Address	Port			
Device Rules (5 rules)										
1	<input type="checkbox"/> Corp-gateSOURCE	Zones: CLA-DMZ-SVRS-INNE ECM-DMZ-SVRS-INNE		China-V4-Netwo	Zones: CLA-DMZ-SVRS-OUT ECM-DMZ-SVRS-OUT		Any	Interface	Not Applicable	Inter NAT Chr Net
2	<input type="checkbox"/> Corp-gateSOURCE	Zones: CLA-DMZ-VDC		China-V4-Netwo	Zones: Corp-DMZ-2 Corp-DMZ-1		Any	Pool Pool Name: PublicChina	Not Applicable	Pool acco DMZ net: chr Pub IP t acco DMZ serv
3	<input type="checkbox"/> Corp-gateSTATIC	Zones: DMZ DMZ-VDC		Not Applicable	Not Applicable		ge1-11	Not Applicable	DHCP	
4	<input type="checkbox"/> Corp-gateDESTINATION	Zones: CLA-DMZ-VDC ECM-DMZ-SVRS-INNE		ALL-WEB_GROUP	Not Applicable		WEB-Rak-2	Any	Same as Original Packet	Pool Pool Name: destination
5	<input type="checkbox"/> Corp-gateDESTINATION	Zones: DMZ DMZ-VDC		India-Network	Not Applicable		WebServer1	8080	Same as Original Packet	Pool Pool Name: Destination1

Save

Discard Changes

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.

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. Create a group policy:

- a. Enter the name of the group policy in the **Name** field.
- b. Enter a description for the group policy in the **Description** field.
- c. Click the **Show Assigned Devices** check box to make the 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 29 on page 105](#).

Figure 29: Create NAT Policy Page

Create NAT Policy

Type: ☒ Group ☐ Device

Name:

Description:

☒ Show Assigned Devices

Select Devices

Filter

Available		Selected
10.205.230.10		10.205.230.1
10.205.230.2		10.205.230.3
10.205.230.4		
10.205.230.5		
10.205.230.6		
10.205.230.7		

- e. Click **Create**.



NOTE: One device can hold configuration data related to one NAT policy only. Hence you cannot share devices for multiple NAT 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 device on which the device policy will be published from the **Device** drop-down menu.
- d. Click **Create**.

Related Documentation

- [Adding Rules to a NAT Policy on page 106](#)
- [Ordering the Rules in a NAT Policy on page 109](#)
- [Publishing NAT Policies on page 110](#)
- [Managing NAT Policies on page 111](#)

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.

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.

The Zone or Interface selector appears.

6. Select the appropriate option from the **Source Traffic Matching Type** drop-down menu.
7. In the zone or interface selector, select the zones or interfaces you want to associate the rule to, from the **Available** column.
8. Click the right arrow in the selector.

The selected zones or interfaces 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.

The zone or interface selector appears.

15. Select the appropriate option from the **Destination Traffic Matching Type** drop-down menu.
16. In the zone or interface selector, select the zones and interfaces you want to associate the rule to, from the **Available** column.
17. Click the right arrow in the selector.

The selected zones or interfaces are now moved to the **Selected** column.

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.

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** drop-down menu appears. You can select the appropriate address from the drop-down menu.

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.

Related Documentation

- [Adding Rules to a NAT Policy on page 106](#)
- [Ordering the Rules in a NAT Policy on page 109](#)
- [Publishing NAT Policies on page 110](#)
- [Managing NAT Policies on page 111](#)

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 104](#)
- [Adding Rules to a NAT Policy on page 106](#)
- [Publishing NAT Policies on page 110](#)
- [Managing NAT Policies on page 111](#)

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.

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 104](#)
- [Adding Rules to a NAT Policy on page 106](#)
- [Ordering the Rules in a NAT Policy on page 109](#)
- [Managing NAT Policies on page 111](#)

Managing NAT Policies

- [Modifying NAT Policies on page 111](#)
- [Deleting NAT Policies on page 112](#)
- [Cloning NAT Policies on page 112](#)
- [Exporting a NAT Policy on page 112](#)
- [Deleting Rules in a NAT Policy on page 113](#)
- [Grouping Rules in a NAT Policy on page 113](#)
- [Enabling/Disabling Rules in a NAT Policy on page 113](#)
- [Assigning Devices to a NAT Policy on page 114](#)
- [Deleting Devices from a NAT Policy on page 114](#)

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.

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 104](#)
- [Adding Rules to a NAT Policy on page 106](#)
- [Ordering the Rules in a NAT Policy on page 109](#)
- [Publishing NAT Policies on page 110](#)

PART 7

Global Search

- [Global Search on page 119](#)

Global Search

- [Global Search on page 119](#)

Global Search

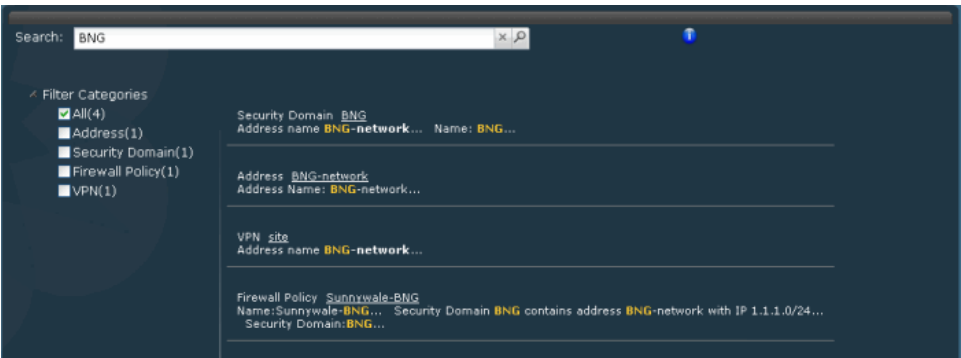
The Security Design home page provides a global search option to find objects and security configurations. You can also click on a search result and navigate to its page.

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 30 on page 119](#).

Figure 30: 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 4 on page 119](#) specifies the objects and configurations that you can search using Global search.

Table 4: Security Design Global Search

Security Design Object/Configuration	Attributes by which Global Search is possible.
--------------------------------------	--

Table 4: 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 123](#)

Downloads

- Downloading the Signature Database on page 123
- Installing the Signature Database on page 125

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 31 on page 123](#).

Figure 31: 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 32 on page 124](#). You can see the active databases that were downloaded earlier.

Figure 32: 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					
Database Version	Publish date	Update Summary	Detectors	Search Version: <input type="text"/>	
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 33 on page 124.

Figure 33: Download Configuration Page

Download Configuration	
Download URL: <input type="text" value="https://services.netscreen.com"/>	
<div> <div>Use Proxy Server</div> <div> <input type="checkbox"/> Enable Proxy: <div> <input type="text" value="Host Name"/> <input type="text" value="Host Port"/> <input type="text" value="User Name"/> <input type="password" value="User Password"/> </div> </div> </div>	
<input checked="" type="checkbox"/> Schedule at a later time <div> Date and time: <input type="text" value="11/24/11"/> <input type="text" value="7:52 AM"/> <input type="text" value="IST"/> </div>	
<input checked="" type="checkbox"/> Repeat <div> <input type="text" value="1"/> <input type="text" value="Hours"/> </div>	
<input type="checkbox"/> End Time <div> <input type="text"/> </div>	
<div> <input type="button" value="Download"/> <input type="button" value="Cancel"/> </div>	

- Enter the URL from where you want to download the AppSecure database in the **Download URL** field.
- Click the **Enable Proxy** check box.
- Enter the hostname in the **Proxy Host Name** field.
- 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 125](#)

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 34 on page 126](#).

Figure 34: 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**.

- Related Documentation**
- [Downloading the Signature Database on page 123](#)

PART 9

IPS Management

- [IPS Management Overview on page 131](#)
- [IPS Management on page 133](#)

CHAPTER 19

IPS Management Overview

- [IPS Management Overview on page 131](#)

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 123](#)
- [Installing the Signature Database on page 125](#)

CHAPTER 20

IPS Management

- [Creating IPS Signatures on page 133](#)
- [Managing IPS Signatures on page 135](#)
- [Creating IPS Signature-sets on page 139](#)
- [Adding Rules to an IPS Signature-set on page 140](#)
- [Managing IPS Signature Sets on page 141](#)
- [Creating IPS Policies on page 143](#)
- [Managing IPS Policies on page 144](#)

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 35 on page 134](#). 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 35: 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 36 on page 134](#).

Figure 36: 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 135](#)

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 136](#)
- [Modifying IPS Signatures on page 136](#)

- [Deleting IPS Signatures on page 136](#)
- [Cloning IPS Signatures on page 137](#)
- [Creating Static Signature Groups on page 137](#)
- [Creating Dynamic Signature Groups on page 138](#)
- [Creating IPS Signature-sets on page 138](#)

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 37 on page 139](#).

Figure 37: 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 140](#)
- [Managing IPS Signature Sets on page 141](#)

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 139](#)
- [Managing IPS Signature Sets on page 141](#)

Managing IPS Signature Sets

- [Deleting IPS Signature-sets on page 141](#)
- [Cloning IPS Signature-sets on page 141](#)
- [Enable or Disable Rules in an IPS Signature-set on page 142](#)

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 Advanced in the device firewall policy. If you want to enable IPS policy creation for a group firewall policy, you would need to:

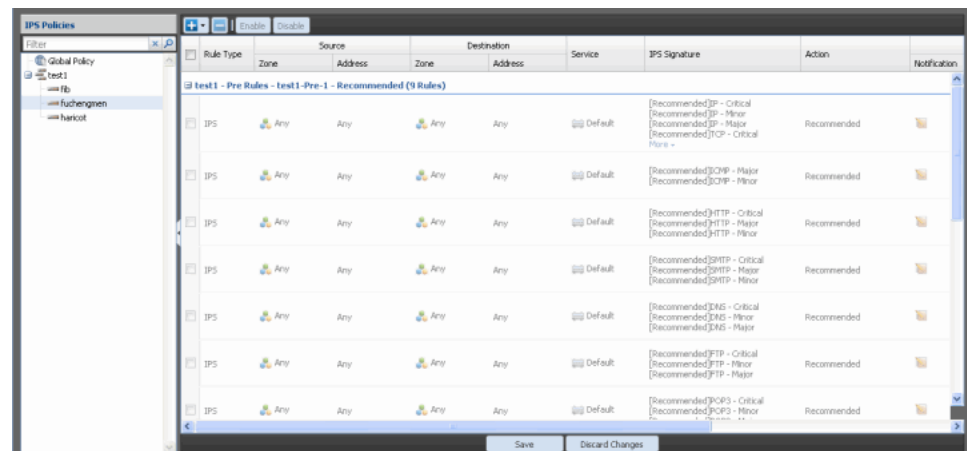
- Enable IPS configuration mode to Advanced for the devices in the group firewall policy.
- Set the **Action** field for the device rule for which you want to enable the firewall policy to **Permit**.
- Select the appropriate IPS signature-set in the IPS field of the device rule.

To create an IPS policy:

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 global policy rules and the device rules for which IPS policy can be created as shown in [Figure 38 on page 143](#).

Figure 38: IPS Policies Tabular View



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 global 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.

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.

**Related
Documentation**

- [Managing IPS Policies on page 144](#)

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 144](#)
2. [Enabling or Disabling Rules in an IPS Policy on page 144](#)

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 149](#)

CHAPTER 21

Security Design Devices

- [Updating Devices with Pending Services on page 149](#)

Updating Devices with Pending Services

To update a device with pending services:

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

The **Security Design Devices** page appears, as shown in [Figure 39 on page 149](#).



Figure 39: Security Design Devices Page

Security Design Devices

Sorted by Name

Select: All | Page | None

Filtered By:

<input type="checkbox"/>	Name	Platform	Licenses	Last Updated	IP Address	Pending Services
<input checked="" type="checkbox"/>	R2-HUB-SRX-102	SRX240B	-	-	10.205.119.102	 Corporate-Policy-Main
<input checked="" type="checkbox"/>	R3-SP1-SRX-103	SRX240B	-	-	10.205.119.103	 Corporate-Policy-Main

10

<

Page

1

of 1

>

>>

<<

<

Displaying 1 - 2 of 2

Show

10

Item

Update

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 40 on page 150](#).

Figure 40: Update Window

Update

☒ Enable policy rematch for SRX-devices

Select service types

☒ Firewall-Policy

☒ VPN

☒ NAT

☒ **Schedule at a later time**

Date and Time: 11/24/11 4:31 PM IST

Update Cancel

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**.



NOTE: Devices will not be listed in the Security Design Devices page until either a security policy or VPN or NAT policy is assigned to the device and a publish or update service is pending.

PART 11

Index

- [Index on page 153](#)

Index

A

address and address groups overview.....	29
address groups	
creating.....	33
deleting.....	35
managing.....	34
modifying.....	35
addresses	
cloning.....	32
creating.....	29
deleting.....	32
exporting.....	33
importing.....	33
managing.....	31
modifying.....	32
application groups	
deleting.....	27
modifying.....	27
application signatures	
creating.....	37
managing.....	39
applications	
deleting.....	25
modifying.....	24

C

conventions	
notice icons.....	xiii
customer support.....	xiv
contacting JTAC.....	xiv

D

Dashboard.....	7
documentation	
comments on.....	xiv
Dynamic signature group	
creating.....	138

F

Firewall policy	
adding rules.....	76
assigning devices.....	87
cloning.....	85
cloning rules.....	85
creating.....	74
deleting.....	84
deleting devices.....	87
deleting rules.....	85
enabling or disabling rules.....	86
exporting.....	85
grouping rules.....	86
modifying.....	84
ordering rules.....	79
overview.....	73
publishing.....	79

G

Global search.....	119
--------------------	-----

I

IPS policy	
creating.....	143
deleting rules.....	144
enabling or disabling rules.....	144
IPS signature	
cloning.....	137
creating.....	133
deleting.....	136
filtering.....	136
modifying.....	136
IPS signature-set	
adding rules.....	140
creating.....	139
managng.....	141
IPsec VPN	
creating.....	92
deleting.....	99
modifying.....	98
modifying endpoint settings.....	99
overview.....	91
publishing.....	96

M

manuals	
comments on.....	xiv

N

NAT

NAT policy	
publishing.....	110
NAT pool	
managing.....	45

NAT policy

adding rules.....	106
assigning devices.....	114
cloning.....	112
creating.....	104
deleting.....	112
deleting devices.....	114
deleting rules.....	113
enabling or disabling rules.....	113
exporting.....	112
grouping rules.....	113
modifying.....	111
ordering rules.....	109
overview.....	103
publishing.....	110

notice icons.....	xiii
-------------------	------

O

Object Builder overview.....	19
------------------------------	----

S

Security design devices

updating.....	149
---------------	-----

Security Design Overview.....	3
-------------------------------	---

security policy profiles

creating.....	48
managing.....	50
overview.....	47

service and service groups overview.....	21
--	----

service groups

creating.....	25
managing.....	26

services

creating.....	22
managing.....	24

Signature database

downloading.....	123
installing.....	125

Static signature group

creating.....	137
---------------	-----

support, technical See technical support

T

technical support

contacting JTAC.....	xiv
----------------------	-----

V

VPN profiles

creating.....	53
overview.....	53