



---

# Junos Space

Object Builder

Release

# 1.3— Beta Draft



---

Published: 2010-06-07

Juniper Networks, Inc.  
1194 North Mathilda Avenue  
Sunnyvale, California 94089  
USA  
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 Designer User Guide*  
Copyright © 2010, Juniper Networks, Inc.  
All rights reserved. Printed in USA.

Revision History  
April 2010—Revision 1, Junos Space Release 1.3— Beta Draft

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

## END USER LICENSE AGREEMENT

### READ THIS END USER LICENSE AGREEMENT ("AGREEMENT") BEFORE DOWNLOADING, INSTALLING, OR USING THE SOFTWARE.

BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE OR OTHERWISE EXPRESSING YOUR AGREEMENT TO THE TERMS CONTAINED HEREIN, YOU (AS CUSTOMER OR IF YOU ARE NOT THE CUSTOMER, AS A REPRESENTATIVE/AGENT AUTHORIZED TO BIND THE CUSTOMER) CONSENT TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT OR CANNOT AGREE TO THE TERMS CONTAINED HEREIN, THEN (A) DO NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND (B) YOU MAY CONTACT JUNIPER NETWORKS REGARDING LICENSE TERMS.

1. **The Parties.** The parties to this Agreement are (i) Juniper Networks, Inc. (if the Customer's principal office is located in the Americas) or Juniper Networks (Cayman) Limited (if the Customer's principal office is located outside the Americas) (such applicable entity being referred to herein as "Juniper"), and (ii) the person or organization that originally purchased from Juniper or an authorized Juniper reseller the applicable license(s) for use of the Software ("Customer") (collectively, the "Parties").

2. **The Software.** In this Agreement, "Software" means the program modules and features of the Juniper or Juniper-supplied software, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller, or which was embedded by Juniper in equipment which Customer purchased from Juniper or an authorized Juniper reseller. "Software" also includes updates, upgrades

and new releases of such software. "Embedded Software" means Software which Juniper has embedded in or loaded onto the Juniper equipment and any updates, upgrades, additions or replacements which are subsequently embedded in or loaded onto the equipment.

3. **License Grant.** Subject to payment of the applicable fees and the limitations and restrictions set forth herein, Juniper grants to Customer a non-exclusive and non-transferable license, without right to sublicense, to use the Software, in executable form only, subject to the following use restrictions:

- a. Customer shall use Embedded Software solely as embedded in, and for execution on, Juniper equipment originally purchased by Customer from Juniper or an authorized Juniper reseller.
- b. Customer shall use the Software on a single hardware chassis having a single processing unit, or as many chassis or processing units for which Customer has paid the applicable license fees; provided, however, with respect to the Steel-Belted Radius or Odyssey Access Client software only, Customer shall use such Software on a single computer containing a single physical random access memory space and containing any number of processors. Use of the Steel-Belted Radius or IMS AAA software on multiple computers or virtual machines (e.g., Solaris zones) requires multiple licenses, regardless of whether such computers or virtualizations are physically contained on a single chassis.
- c. Product purchase documents, paper or electronic user documentation, and/or the particular licenses purchased by Customer may specify limits to Customer's use of the Software. Such limits may restrict use to a maximum number of seats, registered endpoints, concurrent users, sessions, calls, connections, subscribers, clusters, nodes, realms, devices, links, ports or transactions, or require the purchase of separate licenses to use particular features, functionalities, services, applications, operations, or capabilities, or provide throughput, performance, configuration, bandwidth, interface, processing, temporal, or geographical limits. In addition, such limits may restrict the use of the Software to managing certain kinds of networks or require the Software to be used only in conjunction with other specific Software. Customer's use of the Software shall be subject to all such limitations and purchase of all applicable licenses.
- d. For any trial copy of the Software, Customer's right to use the Software expires 30 days after download, installation or use of the Software. Customer may operate the Software after the 30-day trial period only if Customer pays for a license to do so. Customer may not extend or create an additional trial period by re-installing the Software after the 30-day trial period.
- e. The Global Enterprise Edition of the Steel-Belted Radius software may be used by Customer only to manage access to Customer's enterprise network. Specifically, service provider customers are expressly prohibited from using the Global Enterprise Edition of the Steel-Belted Radius software to support any commercial network access services.

The foregoing license is not transferable or assignable by Customer. No license is granted herein to any user who did not originally purchase the applicable license(s) for the Software from Juniper or an authorized Juniper reseller.

4. **Use Prohibitions.** Notwithstanding the foregoing, the license provided herein does not permit the Customer to, and Customer agrees not to and shall not: (a) modify, unbundle, reverse engineer, or create derivative works based on the Software; (b) make unauthorized copies of the Software (except as necessary for backup purposes); (c) rent, sell, transfer, or grant any rights in and to any copy of the Software, in any form, to any third party; (d) remove any proprietary notices, labels, or marks on or in any copy of the Software or any product in which the Software is embedded; (e) distribute any copy of the Software to any third party, including as may be embedded in Juniper equipment sold in the secondhand market; (f) use any 'locked' or key-restricted feature, function, service, application, operation, or capability without first purchasing the applicable license(s) and obtaining a valid key from Juniper, even if such feature, function, service, application, operation, or capability is enabled without a key; (g) distribute any key for the Software provided by Juniper to any third party; (h) use the Software in any manner that extends or is broader than the uses purchased by Customer from Juniper or an authorized Juniper reseller; (i) use Embedded Software on non-Juniper equipment; (j) use Embedded Software (or make it available for use) on Juniper equipment that the Customer did not originally purchase from Juniper or an authorized Juniper reseller; (k) disclose the results of testing or benchmarking of the Software to any third party without the prior written consent of Juniper; or (l) use the Software in any manner other than as expressly provided herein.

5. **Audit.** Customer shall maintain accurate records as necessary to verify compliance with this Agreement. Upon request by Juniper, Customer shall furnish such records to Juniper and certify its compliance with this Agreement.

6. **Confidentiality.** The Parties agree that aspects of the Software and associated documentation are the confidential property of Juniper. As such, Customer shall exercise all reasonable commercial efforts to maintain the Software and associated documentation in confidence, which at a minimum includes restricting access to the Software to Customer employees and contractors having a need to use the Software for Customer's internal business purposes.

7. **Ownership.** Juniper and Juniper's licensors, respectively, retain ownership of all right, title, and interest (including copyright) in and to the Software, associated documentation, and all copies of the Software. Nothing in this Agreement constitutes a transfer or conveyance

of any right, title, or interest in the Software or associated documentation, or a sale of the Software, associated documentation, or copies of the Software.

**8. Warranty, Limitation of Liability, Disclaimer of Warranty.** The warranty applicable to the Software shall be as set forth in the warranty statement that accompanies the Software (the "Warranty Statement"). Nothing in this Agreement shall give rise to any obligation to support the Software. Support services may be purchased separately. Any such support shall be governed by a separate, written support services agreement. TO THE MAXIMUM EXTENT PERMITTED BY LAW, JUNIPER SHALL NOT BE LIABLE FOR ANY LOST PROFITS, LOSS OF DATA, OR COSTS OR PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, THE SOFTWARE, OR ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. IN NO EVENT SHALL JUNIPER BE LIABLE FOR DAMAGES ARISING FROM UNAUTHORIZED OR IMPROPER USE OF ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. EXCEPT AS EXPRESSLY PROVIDED IN THE WARRANTY STATEMENT TO THE EXTENT PERMITTED BY LAW, JUNIPER DISCLAIMS ANY AND ALL WARRANTIES IN AND TO THE SOFTWARE (WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE), INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT DOES JUNIPER WARRANT THAT THE SOFTWARE, OR ANY EQUIPMENT OR NETWORK RUNNING THE SOFTWARE, WILL OPERATE WITHOUT ERROR OR INTERRUPTION, OR WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK. In no event shall Juniper's or its suppliers' or licensors' liability to Customer, whether in contract, tort (including negligence), breach of warranty, or otherwise, exceed the price paid by Customer for the Software that gave rise to the claim, or if the Software is embedded in another Juniper product, the price paid by Customer for such other product. Customer acknowledges and agrees that Juniper has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the Parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the Parties.

**9. Termination.** Any breach of this Agreement or failure by Customer to pay any applicable fees due shall result in automatic termination of the license granted herein. Upon such termination, Customer shall destroy or return to Juniper all copies of the Software and related documentation in Customer's possession or control.

**10. Taxes.** All license fees payable under this agreement are exclusive of tax. Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software. If applicable, valid exemption documentation for each taxing jurisdiction shall be provided to Juniper prior to invoicing, and Customer shall promptly notify Juniper if their exemption is revoked or modified. All payments made by Customer shall be net of any applicable withholding tax. Customer will provide reasonable assistance to Juniper in connection with such withholding taxes by promptly: providing Juniper with valid tax receipts and other required documentation showing Customer's payment of any withholding taxes; completing appropriate applications that would reduce the amount of withholding tax to be paid; and notifying and assisting Juniper in any audit or tax proceeding related to transactions hereunder. Customer shall comply with all applicable tax laws and regulations, and Customer will promptly pay or reimburse Juniper for all costs and damages related to any liability incurred by Juniper as a result of Customer's non-compliance or delay with its responsibilities herein. Customer's obligations under this Section shall survive termination or expiration of this Agreement.

**11. Export.** Customer agrees to comply with all applicable export laws and restrictions and regulations of any United States and any applicable foreign agency or authority, and not to export or re-export the Software or any direct product thereof in violation of any such restrictions, laws or regulations, or without all necessary approvals. Customer shall be liable for any such violations. The version of the Software supplied to Customer may contain encryption or other capabilities restricting Customer's ability to export the Software without an export license.

**12. Commercial Computer Software.** The Software is "commercial computer software" and is provided with restricted rights. Use, duplication, or disclosure by the United States government is subject to restrictions set forth in this Agreement and as provided in DFARS 227.7201 through 227.7202-4, FAR 12.212, FAR 27.405(b)(2), FAR 52.227-19, or FAR 52.227-14(ALT III) as applicable.

**13. Interface Information.** To the extent required by applicable law, and at Customer's written request, Juniper shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Juniper makes such information available.

**14. Third Party Software.** Any licensor of Juniper whose software is embedded in the Software and any supplier of Juniper whose products or technology are embedded in (or services are accessed by) the Software shall be a third party beneficiary with respect to this Agreement, and such licensor or vendor shall have the right to enforce this Agreement in its own name as if it were Juniper. In addition, certain third party software may be provided with the Software and is subject to the accompanying license(s), if any, of its respective owner(s). To the extent portions of the Software are distributed under and subject to open source licenses obligating Juniper to make the source code for such portions publicly available (such as the GNU General Public License ("GPL") or the GNU Library General Public License ("LGPL")), Juniper will make such source code portions (including Juniper modifications, as appropriate) available upon request for a period of up to three years from the date of distribution. Such request can be made in writing to Juniper Networks, Inc., 1194 N. Mathilda Ave., Sunnyvale, CA

94089, ATTN: General Counsel. You may obtain a copy of the GPL at <http://www.gnu.org/licenses/gpl.html>, and a copy of the LGPL at <http://www.gnu.org/licenses/lgpl.html>.

15. **Miscellaneous.** This Agreement shall be governed by the laws of the State of California without reference to its conflicts of laws principles. The provisions of the U.N. Convention for the International Sale of Goods shall not apply to this Agreement. For any disputes arising under this Agreement, the Parties hereby consent to the personal and exclusive jurisdiction of, and venue in, the state and federal courts within Santa Clara County, California. This Agreement constitutes the entire and sole agreement between Juniper and the Customer with respect to the Software, and supersedes all prior and contemporaneous agreements relating to the Software, whether oral or written (including any inconsistent terms contained in a purchase order), except that the terms of a separate written agreement executed by an authorized Juniper representative and Customer shall govern to the extent such terms are inconsistent or conflict with terms contained herein. No modification to this Agreement nor any waiver of any rights hereunder shall be effective unless expressly assented to in writing by the party to be charged. If any portion of this Agreement is held invalid, the Parties agree that such invalidity shall not affect the validity of the remainder of this Agreement. This Agreement and associated documentation has been written in the English language, and the Parties agree that the English version will govern. (For Canada: Les parties aux présentes confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattache, soient rédigés en langue anglaise. (Translation: The parties confirm that this Agreement and all related documentation is and will be in the English language)).



# Table of Contents

<b>Chapter 1</b>	<b>Security Whiteboard</b> . . . . .	<b>1</b>
	Security Whiteboard Overview . . . . .	1
<b>Chapter 2</b>	<b>Security Topology Designer</b> . . . . .	<b>3</b>
	Security Topology Overview . . . . .	3
	Creating a Security Topology . . . . .	4
	Dragging and Dropping Security Devices . . . . .	6
	Connecting Security Devices . . . . .	7
	Dragging and Dropping Addresses . . . . .	8
	Associating Addresses With Security Devices . . . . .	8
	Dragging and Dropping Security Domains . . . . .	8
	Associating Addresses With Security Domains . . . . .	9
	Removing Addresses from a Security Domain . . . . .	9
	Creating Address Groups . . . . .	9
	Creating Device Groups . . . . .	9
	Removing Devices from a Device Group . . . . .	10
	Searching for Devices, Addresses, and Security Domains in the Topology . . . . .	10
	Creating Group Links on Device Groups . . . . .	10
	Adding Addresses and Security Domains Using CSV Import . . . . .	11
<b>Chapter 3</b>	<b>Security Policy Profiles</b> . . . . .	<b>13</b>
	Security Policy Profiles Overview . . . . .	13
	Creating Security Policy Profiles . . . . .	14
	Managing Security Policy Profiles . . . . .	17
	Viewing the Details of a Security Policy Profile . . . . .	17
	Modifying a Security Policy Profile . . . . .	18
	Copying a Security Policy Profile . . . . .	19
	Deleting a Security Policy Profile . . . . .	19
	Searching for a Security Policy . . . . .	20
<b>Chapter 4</b>	<b>Security Policy Designer</b> . . . . .	<b>21</b>
	Security Policies Overview . . . . .	21
	Creating Security Policies . . . . .	22
	Managing Security Policies . . . . .	27
	Viewing the Details of a Security Policy . . . . .	27
	Modifying a Security Policy . . . . .	27
	Deleting a Security Policy . . . . .	28
	Searching for a Security Policy . . . . .	28
	Deploying Security Policies . . . . .	28

<b>Chapter 5</b>	<b>VPN Proposals</b> . . . . .	<b>31</b>
	VPN Proposals Overview . . . . .	31
	Creating VPN Proposals . . . . .	32
	Managing VPN Proposals . . . . .	36
	Viewing the Details of a VPN Proposal . . . . .	36
	Modifying a VPN Proposal . . . . .	37
	Deleting a VPN Proposal . . . . .	38
	Copying a VPN Proposal . . . . .	39
	Searching for a VPN Proposal . . . . .	39
<b>Chapter 6</b>	<b>VPN Profiles</b> . . . . .	<b>41</b>
	VPN Profiles Overview . . . . .	41
	Creating VPN Profiles . . . . .	42
	Managing VPN Profiles . . . . .	48
	Viewing the Details of a VPN Profile . . . . .	48
	Modifying a VPN Profile . . . . .	49
	Deleting a VPN Profile . . . . .	50
	Copying a VPN Profile . . . . .	51
	Searching for a VPN Profile . . . . .	51
<b>Chapter 7</b>	<b>IPSec VPN</b> . . . . .	<b>53</b>
	IPSec VPNs Overview . . . . .	53
	Creating IPSec VPNs . . . . .	53
	Site-To-Site . . . . .	55
	Hub-And-Spoke . . . . .	56
	Managing IPSec VPNs . . . . .	57
	Modifying a IPSec VPN . . . . .	58
	Deleting an IPSec VPN . . . . .	58
	Deploying IPSec VPNs . . . . .	59
<b>Chapter 8</b>	<b>Index</b> . . . . .	<b>63</b>
	Index . . . . .	65



## CHAPTER 1

# Security Whiteboard

- [Security Whiteboard Overview on page 1](#)

### Security Whiteboard Overview

---

The Security Whiteboard workspace in Security Design allows you to create a security topology, IPSec VPNs and security policies.

The Security Topology Designer allows you to create a graphical view of the security aspect of the network. This serves as a base to create IPSec VPNs and security policies on the network.

You can also create Hub-And-Spoke and Site-To-Site VPNs on your security topology. The following objects are used to create an IPSec VPN:

- A VPN proposal which defines a set of IKE proposals and IPSec proposals used for an IPSec VPN
- A VPN profile which defines a VPN proposal, IKE settings, IPSec settings, and connectivity parameters used for an IPSec VPN

The Security Policy Designer Whiteboard is used to create security policies between multiple security domains. You can associate the applications hosted by a security domain and the addresses associated with the security domain on-the-fly.

#### Related Topics

- [Security Topology Overview on page 3](#)
- [Security Policy Profiles Overview on page 13](#)
- [Security Policies Overview on page 21](#)
- [VPN Proposals Overview on page 31](#)
- [VPN Profiles Overview on page 41](#)
- [IPSec VPNs Overview on page 53](#)



## CHAPTER 2

# Security Topology Designer

- Security Topology Overview on page 3
- Creating a Security Topology on page 4

### Security Topology Overview

---

Security topology is a logical map, which depicts the inter-connectivity between security devices, networks that are protected by security devices, and security domains that host these networks. Security topology serves as a foundation to create IPSec VPNs on your network and configure firewall policies on your security devices.

Security Topology Designer allows you to drag and drop security devices, networks, and security domains on the Security Topology Whiteboard. You can create links between networks and security devices and also between security devices. The Security Topology Designer also allows you to associate multiple networks to a security domain. This helps you to logically partition the network into various security domains based on your organization's security requirements.

A toolbar on the Security Topology Designer provides the functionality to save and edit a topology design, delete the components of a topology, and shrink the entire topology to a visible area in case you host a large topology. The security devices, security domains, and addresses can be chosen from their individual object chooser panels. You can configure the interfaces used for communication once the components are linked in the topology design.

Security Topology Designer includes the following functionalities to make your topology design flexible and easy:

- Device groups
- Address groups
- Aggregate links between security devices
- CSV Import of addresses and security domains
- Search functionality to search specific objects in the topology

**Related Topics**   • Creating a Security Topology on page 4

## Creating a Security Topology

---

To navigate to the Security Topology Designer Whiteboard, perform the following steps:






1. From the **Security Design** task ribbon, select **Security Whiteboard > Security Topology**. The **Security Topology Designer Whiteboard** is displayed, as shown in Figure 1 on page 5.

Figure 1: Security Topology Designer Whiteboard



The toolbar on the left displays a set of functionalities used to design the security topology, as listed in Table 1 on page 5.

Table 1: Security Topology Designer Toolbar Icons

Toolbar Icon	Icon Name	Description
	Show All	Used to fit the topology graph on the Topology Designer Whiteboard. This shrinks the entire topology to a visible area
	Create Link	Used to create links between security devices or between a device and an address in the topology design
	Save Topology	Used to save a topology design
	Modify	Used to modify the selected item of a topology design. For example, modifying the interface on a link or modifying an address or a domain
	Delete	Used to delete links, security devices, addresses, or security domains in the topology design

The Object chooser panel on the right displays the addresses, security devices and security domains that are available for creating the security topology.

The Select:Page and Select:All links help you to select multiple objects at one go. The Clear:Page and Clear:All links help you to de-select the objects that you have selected.

You can use the Search option, next to the Object chooser panel to search for specific security devices, addresses, security domains, address groups, and device groups used to create the topology.

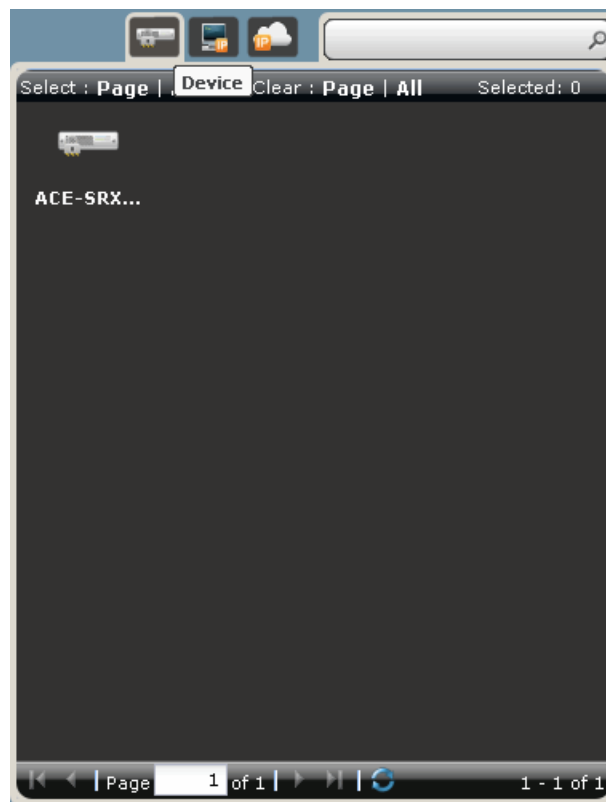
The devices, addresses and security domains can be dragged and dropped and inter-connected in the following ways:

1. Dragging and Dropping Security Devices on page 6
2. Connecting Security Devices on page 7
3. Dragging and Dropping Addresses on page 8
4. Associating Addresses With Security Devices on page 8
5. Dragging and Dropping Security Domains on page 8
6. Associating Addresses With Security Domains on page 9
7. Removing Addresses from a Security Domain on page 9
8. Creating Address Groups on page 9
9. Creating Device Groups on page 9
10. Removing Devices from a Device Group on page 10
11. Searching for Devices, Addresses, and Security Domains in the Topology on page 10
12. Creating Group Links on Device Groups on page 10
13. Adding Addresses and Security Domains Using CSV Import on page 11

## Dragging and Dropping Security Devices

1. From the Object chooser panel, click the **Device** object icon. All devices available to create the security topology are listed in the collapsible Device chooser, as shown in Figure 2 on page 7.

Figure 2: Security Topology Designer : Selecting Devices



NOTE: Only security devices is shown in Device chooser.

2. Drag and drop security devices to the Security Topology Whiteboard from the Device chooser panel.

### Connecting Security Devices

1. Select the Create Link icon from the toolbar and draw a line between security devices. This line represents the link between these security devices.  
  
The link created in between security domains is a logical link which may pass through other networking devices like routers and switches.
2. Right-click the link between the security devices and select **Configure Interface** from the contextual menu. The **Link Properties** window is displayed.
3. In the **Link Properties** window, add an interface from the **Available Interfaces** section to the **Selected Interfaces** section on one end of the link.
4. Repeat Step 2 and 3 for the other end of the link and click **Configure**.



NOTE: The overlay icons indicate if the device interfaces are configured. For example, a yellow triangle with a black exclamation specifies that the device interface is not configured and a green circle with a white check mark specifies that the device interface is configured.

## Dragging and Dropping Addresses

1. From the Object chooser panel select the **Address** object Icon. All address groups available to create a security topology are listed in the collapsible Address chooser.
2. Drag and drop addresses/address groups to the Security Topology Whiteboard from the Address chooser panel.



NOTE: You can use the Internet address object to define a topology which is spread across multiple branches or locations. If the branches are connected through the internet, you can use the Internet address object as a common point for all your branch topologies to connect to each other and constitute the entire topology.

## Associating Addresses With Security Devices

1. Select the Create Link icon from the toolbar and draw a line between the security device and the address object. This line represents the link between the security device and the address object.  
  
The link created in between a security domains and an address is a logical link which may pass through other networking devices like routers and switches.
2. Right-click the link between a security device and address object and select **Configure Interface** from the contextual menu. The **Link Properties** window is displayed.
3. In the **Link Properties** window, add an interface from the **Available Interfaces** section to the **Selected Interfaces** section on the endpoint which has a device.
4. Click **Configure**.

This link specifies that the address is protect by the firewall through the specified interface.

## Dragging and Dropping Security Domains

1. From the Object chooser panel select the **Security Domain** object Icon. All security domains available to create a security topology are listed in the collapsible Security Domain chooser.
2. Drag and drop security domains to the Security Topology Whiteboard from the Security Domain chooser panel.



## Associating Addresses With Security Domains

1. Drag and drop addresses/address groups from the Address chooser on top of the security domain to associate the addresses/address groups to the security domain.
2. To view the addresses/address groups associated with a security domain, click the "+" symbol on the top left corner of the security domain in the Topology Designer Whiteboard. A blue rectangular box is displayed; this box bounds all addresses/address groups associated to this security domain.



**NOTE:** You can also drag and drop the addresses/address groups that are already included in the topology.

## Removing Addresses from a Security Domain

1. Right-click on the address which you want to remove from the domain.
2. Select the **Detach Address from Security Domain** option in the contextual menu. This will remove the address from the domain.

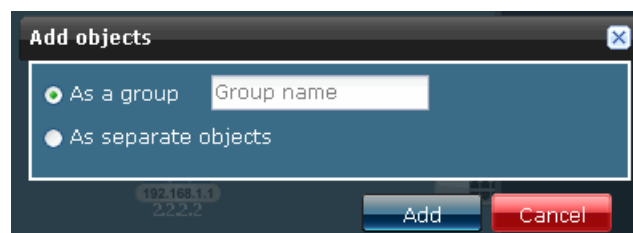
## Creating Address Groups

1. Select multiple addresses from the Address chooser and drag and drop them to the Security Topology Whiteboard. The **Add Objects** window is displayed.
2. Enter a name for the address group in the **As a Group** field.
3. Click **Add**. The address group is displayed on the Security Topology Whiteboard.

## Creating Device Groups

1. Select multiple devices from the Device chooser and drag and drop them to the Security Topology Whiteboard. The **Add Objects** window is displayed, as shown in Figure 3 on page 9.

**Figure 3: Add Objects Window**



2. Enter a name for the device group in the **As a Group** field.
3. Click **Add**. The device group is displayed on the Security Topology Whiteboard.
4. To view the devices associated with a device group, click the "+" symbol on the top left corner of the device group in the Topology Designer Whiteboard. A blue

rectangular box is displayed; this box bounds all devices associated with this device group.



NOTE: You can also add devices that are already a part of the security topology to a device group.

## Removing Devices from a Device Group

1. Right-click on the device you want to delete from the device group.
2. Select the **Detach Device from Device Group** option from the contextual menu.  
This will remove the device from the device group.

1.

## Searching for Devices, Addresses, and Security Domains in the Topology

1. Enter the name of the device, address, or security domain you want to search, in the search field, next to the object chooser icons.
2. Click the magnifying glass icon next to the search field.  
All devices, addresses, or security domains that match the search criterion will be highlighted, on the Topology Whiteboard.



NOTE: You can also use search expressions like \*, + and ? to perform a search.



NOTE: If your search criteria corresponds to an address within a domain, address within an address group, or a device within a device group, the group hosting the object searched for expands and highlights the object.

## Creating Group Links on Device Groups

1. Select the Create Link icon from the toolbar and draw a line between the device group and the device you want to link. The interfaces that are shown on the device group is a union of all available interfaces in the device group.
2. Right-click the link between the device group and the device and select **Configure Interface** from the contextual menu. The **Link Properties** window is displayed.



NOTE: If you use the **Configure Interface** option for the entire device group, all device interfaces in the device group will be configured on a global basis. To configure unique interfaces for each device on the device group, expand the device group by clicking the "+" symbol on the top left corner of the device group, and configure the interface for each device.

3. In the **Link Properties** window, add an interface from the **Available Interfaces** section to the **Selected Interfaces** section on the endpoint which has a device.
4. Repeat Step 2 and 3 for the other end of the link and click **Configure**. This link is displayed with a different color.



**NOTE:** The number of individual links configured can be viewed by hovering on the link.

## Adding Addresses and Security Domains Using CSV Import

1. Right-click the Topology Designer Whiteboard and select **Import Address/Domain** from the contextual menu. The **Select CSV File** window is displayed.
2. Click **Browse** and upload the CSV file from your storage location. This CSV file contains the addresses associated to the respective devices and security domains. The addresses and security domains uploaded are available in the respective object chooser panels.
3. You can also choose to view a sample CSV file by clicking the **View Sample CSV** link on the **Select CSV File** window.

The fields available in the sample CSV file are as shown in Table 2 on page 11

**Table 2: Adding Addresses and Security Domains Using CSV Import**

Field Name	Field Description
Name	This field specifies the name of the address object.
Description	This field specifies the description of the address object.
Type	This field specifies the type of address you want to add to the topology.
IP Address	This field specifies the IP address of the network. It is used if the address type is IP Address.
Subnet Mask	This field specifies the subnet mask of the network specified by the address. This field is used if the address type is a Network.
IP Range Min	This field specifies the first IP address in the range of IP addresses specified. It is used if the address type is IP Range.
IP Range Max	This field specifies the last IP address in the range of IP addresses specified. It is used if the address type is IP Range.
Hostname	This field specifies the hostname, if the address type is a Hostname.
Security Domain	This field specifies the security domain to which the address is associated.
Device	This field specifies the security device which you want to use to protect the network.
Interface	This field specifies the interface through which the address is associated with the security device.



NOTE: You cannot upload address groups using the CSV import functionality. The types of addresses that are supported are IP address, Network, IP range and Hostname.



NOTE: All devices that are associated to the addresses in the CSV file should exist in the Device chooser panel.

**Related Topics**

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

## CHAPTER 3

# Security Policy Profiles

- Security Policy Profiles Overview on page 13
- Creating Security Policy Profiles on page 14
- Managing Security Policy Profiles on page 17

### Security Policy Profiles Overview

---

You can use the Policy Profile Wizard to create an object that specifies the basic settings of a security policy. The basic settings that can be configured using the Policy Profile Wizard include:

- Log options — the options include:
  1. Log at session initiation
  2. Log at the close of a session
  3. Enable counting for the number of packets, bytes, and sessions that enter the firewall for a given policy.
- Firewall authentication schemes — the authentication schemes include:
  1. Pass through authentication
  2. Web authentication
- Traffic redirection options — the traffic redirection options include:
  1. No traffic redirection
  2. Redirect Wx — Wx redirection for packets that arrive from the LAN
  3. 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. This object can be used to create security policies.

Junos Space provides two Juniper Networks defined policy profiles which include:

1. All logging enabled — this policy profile has all logging options 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.

2. All logging disabled — this policy profile has all logging options disabled.



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

#### Related Topics

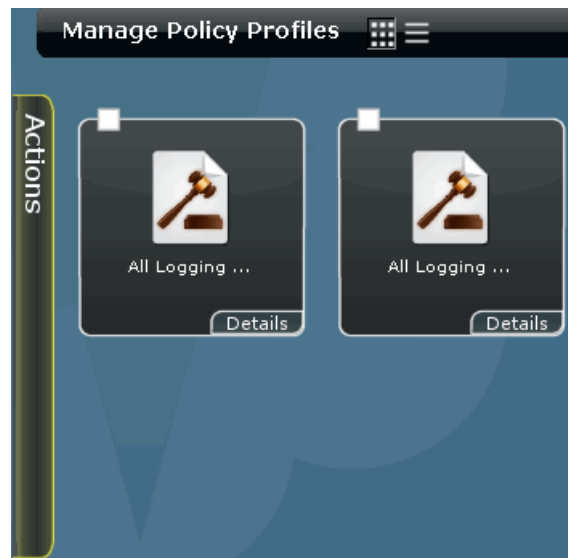
- Creating Policy Profiles on page 14
- Managing Security Policy Profiles on page 17

## Creating Security Policy Profiles

To create a new security policy profile, perform the following steps:

1. From the **Security Design** task ribbon, select **Security Whiteboard** > **Security Policy** > **Policy Profiles**. The **Manage Policy Profiles** inventory panel is displayed with the icons for all the policy profiles as shown in Figure 4 on page 14. The first two policy profiles listed here are Juniper Networks defined policy profiles.

**Figure 4: Manage Policy Profiles Inventory Panel**



2. From the task ribbon, select the **Create Profile** icon. The **New Policy Profile** window is displayed as shown in Figure 5 on page 15.

Figure 5: New Policy Profile Window

**New Policy Profile**

Name:

Description:

**Logging** Authentication Redirect

☐ Log At Session Init      Alarm Threshold:  Bytes/Second

☐ Log At Session       Kilobytes/Minute

☐ Enable Count     

Create Cancel

3. In the **Name** field, enter a name for the new policy profile.
4. In the **Description** field, enter a description for the new policy profile.
5. The **Logging** section of the **New Policy Profile** window allows you to 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. 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
6. In the **Firewall Authentication** section of the **New Policy Profile** window, enter the following details, as shown in Figure 6 on page 16:

Figure 6: New Policy Profile: Firewall Authentication Section

New Policy Profile

Name:

Description:

Logging Authentication Redirect

Pass Through Client:

Web Authentication Client:

Create Cancel

- a. In the **Pass Through Client Name** field enter the host name or IP address of the client used to perform Pass Through authentication.
  - b. In the **Web Authentication Client Name** field enter the host name or IP address of the client used to perform Web authentication.
7. The **Redirect** section of the **New Policy Profile** window allows you to configure the traffic redirection options for this policy profile. You can configure the traffic redirection options, as shown in Figure 7 on page 16:

Figure 7: New Policy Profile: Redirect Section

New Policy Profile

Name:

Description:

Logging Authentication Redirect

Redirect: ☒ None  
☐ Redirect Wx  
☐ Reverse Redirect Wx

Create Cancel

- a. Select the **None** check box if you want traffic to be redirected.



- b. Select the **Redirect Wx** check box if you want to enable Wx redirection for packets that arrive from the LAN.
  - c. Select the **Reverse Redirect Wx** check box if you want to enable Wx redirection for the reverse flow of packets that arrive from the WAN.
8. Click **Create**. The new security policy profile you have created is displayed in the **Manage Policy Profiles** inventory panel.

- Related Topics**
- Security Policy Profiles Overview on page 13
  - Managing Security Policy Profiles on page 17

## Managing Security Policy Profiles

---

You can view, modify, copy or delete security policy profiles listed in the **Manage Policy Profiles** inventory panel. To open the **Manage Policy Profiles** inventory panel:

1. From the **Security Design** task ribbon, select **Security Whiteboard > Security Policy > Policy Profiles**. The **Manage Policy Profiles** inventory panel is displayed. All security policy profiles created is listed by default, in the graphical view.

The tasks that can be performed in the **Manage Policy Profiles** space include:

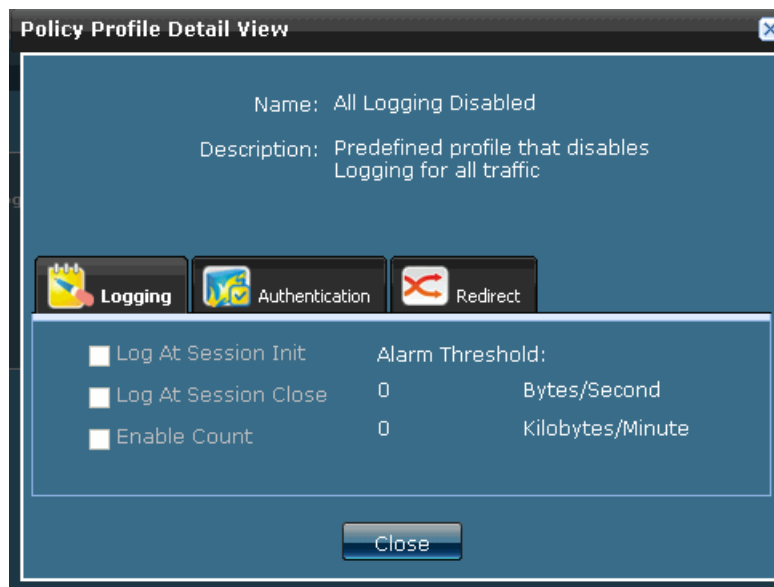
1. Viewing the Details of a Security Policy Profile on page 17
2. Modifying a Security Policy Profile on page 18
3. Copying a Security Policy Profile on page 19
4. Deleting a Security Policy Profile on page 19
5. Searching for a Security Policy on page 20

## Viewing the Details of a Security Policy Profile

To view the details of a security policy profile, perform the following steps:

1. From the **Security Design** task ribbon, select **Security Whiteboard > Security Policy > Policy Profiles**. The **Manage Policy Profiles** inventory panel is displayed.
2. Double-click the icon for the security policy profile whose details you intend to view. The details of the security policy profile are displayed in the **Policy Profile Detail View** window as shown in Figure 8 on page 18.

Figure 8: Policy Profile Detail View Window



3. Click **Close**.

## Modifying a Security Policy Profile

To modify a security policy profile you have created, perform the following steps:

1. From the **Security Design** task ribbon, select the **Security Whiteboard > Security Policy > Policy Profiles**. The **Manage Policy Profiles** inventory panel is displayed.
2. Right-click the security policy profile which you want to modify and select **Modify Policy Profile** from the contextual menu. The **Modify Policy Profile** window is displayed. 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 choose to modify a policy profile using the **Actions Panel**. To do so:

1. Select the check box on the left corner of the policy profile you want to modify.
2. Click the **Actions Panel** located on the left corner of the inventory panel and select **Modify Policy Profile**.
3. Make necessary changes to the policy profile and click **Modify**.

## Copying a Security Policy Profile

To copy a security policy profile you have created, perform the following steps:

1. From the **Security Design** task ribbon, select the **Security Whiteboard > Security Policy > Policy Profiles**. The **Manage Policy Profiles** inventory panel is displayed.
2. Right-click the security policy profile which you want to copy and select **Copy Policy Profile** from the contextual menu. The **Copy Policy Profile** window is displayed.
3. In the **Name** field, enter a name for the new security policy profile.
4. Edit the other fields of the security policy profile if you intend to do so.
5. Click **Create** to create a new security policy profile. The new security policy profile you have created is displayed in the **Manage Policy Profiles** Inventory panel.



NOTE: You can also choose to copy a policy profile using the **Actions Panel**. To do so:

1. Select the check box on the left corner of the policy profile you want to copy.
2. Click the **Actions Panel** located on the left corner of the inventory panel and select **Copy Policy Profile**.
3. Make necessary changes to the policy profile and click **Create**.

## Deleting a Security Policy Profile

To delete a security policy profile you have created, perform the following steps:

1. From the **Security Design** task ribbon, select the **Security Whiteboard > Security Policy > Policy Profiles**. The **Manage Policy Profiles** inventory panel is displayed.
2. Right-click the security policy profile which you want to delete and select **Delete Policy Profile** from the contextual menu. The **Delete Policy Profile** window is displayed.
3. Select the security policy profile you want to delete and click **Delete**.



NOTE: You can also choose to delete a policy profile using the **Actions Panel**. To do so:

1. Select the check box on the left corner of the policy profile you want to delete.
2. Click the **Actions Panel** located on the left corner of the inventory panel and select **Delete Policy Profile**.
3. Select the policy profile you want to delete and click **Delete**.

## Searching for a Security Policy

To search for a security policy profile you have created, perform the following steps:

1. From the **Security Design** task ribbon, select the **Security Whiteboard > Security Policy > Policy Profiles**. The **Manage Policy Profiles** inventory panel is displayed.
2. Enter the name of security policy profile you want to search, in the **Search** field.
3. Click the Magnifying glass icon next to **Search** field. The **Manage Policy Profiles** inventory panel is populated with the security policy profiles matching your search criterion.

- Related Topics**
- Security Policy Profiles Overview on page 13
  - Creating Policy Profiles on page 14

## CHAPTER 4

# Security Policy Designer

- Security Policies Overview on page 21
- Creating Security Policies on page 22
- Managing Security Policies on page 27
- Deploying Security Policies on page 28

### Security Policies Overview

---

You can use the Policy Designer Whiteboard to create security policies between security domains. A security policy is a collection of rules defined to permit, or deny application data between two security domains. Security policies are used to control the flow of application data from one security domain to another by specifying the applications that are allowed or denied to pass data to a security domain. The direction in which the application data is allowed or denied i.e. from domain 1 to domain 2 or domain 2 to domain 1 can also be specified.

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

The advanced settings of a security policy include rule action (permit/deny) and rule direction (both directions/one direction) for a security policy.

The steps used to configure a security policy using the Policy Designer Whiteboard include:

1. Drag and drop the security domains which are the end points of a security policy.
2. Create a policy between the security domains which are the end points of a security policy.
3. Configure a security policy that defines rules to allow, or deny application data in specific directions.

#### Related Topics

- Creating Security Policies on page 22
- Deploying Security Policies on page 28
- Managing Security Policies on page 27

## Creating Security Policies

To create security policies between security domains, perform the following steps:





1. From the **Security Design** task ribbon, select **Security Whiteboard > Security Policy Designer**. The **Security Policy Designer Whiteboard** is displayed, as shown in Figure 9 on page 22.

Figure 9: Security Policy Designer Whiteboard



The toolbar on the left displays a set of functionalities used to design security policies, as listed in Table 3 on page 22.

Table 3: Security Policy Designer Toolbar Icons

Toolbar Icon	Icon Name	Description
	Show All	Used to fit the policy graph on the Policy Designer Whiteboard
	Create Policy	Used to create a policy between security domains
	Save Coordinates	Used to save a security policy design
	Delete	Used to delete security policies or security domains in the security policy design

2. From the right panel, click the Security Domains object icon. All security domains available to create a security policy are listed in the Security Domain chooser.
3. Drag and drop the first security domain that is a part of the security policy to the Policy Designer Whiteboard.

4. Drag and drop the second security domain that is a part of the security policy to the Policy Designer Whiteboard.
5. Select the Create Policy icon and draw a line between security domains. This line represents the security policy that is created between the security domains.
6. To configure a policy between the security domains, right-click the line and select **Create Policy** from the contextual menu. The **Create Policy** window is displayed as shown in Figure 10 on page 23.

Figure 10: Create Policy Window

**Create Policy**

Engg HR

Name:

Description:

Profile: All Logging Enabled ▼

**Rules**

Direction	Applications	Action	Settings
	rtsp tftp tacacs-ds tacacs bootpc		
	ftp netbios-session smtp		
	telnet ssh		

7. In the **Name** field, enter an appropriate name for this security policy.
8. In the **Description** field, enter a description for this security policy.
9. Select an appropriate policy profile from the **Profile** field.
10. The **Rules** section of the **Create Policy** window lists the rules that are a part of the security domain. The **Rules** section displays the following attributes for each rule displayed:
  - Whether the rule is inherited from the security domains or added from the **Rules** section
  - Direction/s in which the traffic flows

- Applications that are a part of the rule
- Whether traffic is permitted or denied in the given direction/s
- Whether the policy profile is customized for a specific rule



**NOTE:** If you inherit a rule from a security domain, the rule displays an icon on the left. If you add a rule from the Rules section, this icon is not displayed.

You can choose to add, edit or delete a rule in the table.

- To add a rule:
  - Select the **Add** icon. The **Add Rule** window is displayed, as shown in Figure 11 on page 24.

Figure 11: Add Rule Window



- In the **Description** field, enter an appropriate description.
- Select the application/s from the **Available** section of the dialog box and click the Add icon. The application/s you have selected is/are displayed in the **Selected** section of this dialog box.



4. Select the direction of traffic from the **Direction** section of the **Add Rule** window.
5. Select the action to be performed on the traffic from the **Action** section of the **Add Rule** window.
6. To make any specific changes to the policy profile settings used in this rule, click **Advanced Setting**. The **Rule Details** window refreshes to display the policy profile settings used for this rule.
7. Select the **Use Custom Settings for This Rule** check box to ensure that the changes made to the policy profile settings in the **Rule Details** window affect only this rule.
8. Click **Add**.



NOTE: A rule that is added in the **Create Policy** window displays a red triangle at top left corner of the cell.



NOTE: If any changes are made to the policy profile for a specific rule, an icon is displayed in the **Settings** column of the rule.

- b. To delete a rule:
  1. Select the rule you want to delete and click the **Delete** icon.
- c. To edit a rule:
  1. Select the rule you want to edit and click the **Edit** icon. The **Rule Details** window is displayed.
  2. Make appropriate changes to the direction of traffic in the **Direction** section.
  3. Make appropriate changes to the action performed by the security policy in the **Action** section.
  4. To add more applications to this rule move the applications from the **Available** section to the **Selected** section.
  5. To make any specific changes to the policy profile settings used in this rule, click **Advanced Setting**. The **Rule Details** window refreshes to display the policy profile settings used for this security policy.
  6. Select the **Use Custom Settings for This Rule** check box to ensure that the changes made to the policy profile settings in the **Rule Details** window affect only this rule.
  7. Make appropriate changes to the policy profile settings and click **OK**. The **Settings** column on the rule that was edited displays the section of the policy profile that was edited. For example, if you made changes to the

**Firewall Authentication** section of the policy profile the **Settings** column displays **Authentication**.



NOTE: You cannot change the action or the direction of traffic for rules that are inherited from a security domain.

11. Click **Create**. The new security policy you have created is displayed in the **Manage Policies** inventory panel
12. To add more security domains to this security policy design, drag and drop security domains to the Policy Designer Whiteboard. Repeat Steps 4 through 10.



NOTE: You can deploy or delete a security policy from the Policy Designer Whiteboard. To deploy a security policy:

1. Right-click the security policy between security domains and select **Deploy Policy** from the contextual menu. To know more about how to deploy a security policy, click “Deploying Security Policies” on page 28.

To delete a security policy:

1. Right-click the security policy between security domains and select **Delete Policy** from the contextual menu. To know more about how to delete a security policy, click “Managing Security Policies” on page 27.



NOTE: You can clear a security policy design from the Policy Designer Whiteboard. You should first delete the security policy to be able to delete the security domains that are the end points of a security policy. To do so, perform the following steps:

1. Select the security policy between the security domains that you want to delete.
2. Select the **Delete** icon from the Policy Designer toolbar.
3. Select one of the two security domains that are the end points of the security policy.
4. Select the **Delete** icon from the Policy Designer toolbar.
5. Select the other security domain that is the end point of the security policy.
6. Select the **Delete** icon from the Policy Designer toolbar.

---

#### Related Topics

- Security Policies Overview on page 21
- Deploying Security Policies on page 28
- Managing Security Policies on page 27

## Managing Security Policies

You can view, modify or delete security policies listed in the **Manage Policies** inventory panel. To open the **Manage Policies** inventory panel:

1. From the **Security Design** task ribbon, select **Security Whiteboard > Security Policy**. The **Manage Policies** inventory panel is displayed. All security policies created is listed by default, in the tabular view.

The tasks that can be performed in the **Manage Policies** space include:

1. Viewing the Details of a Security Policy on page 27
2. Modifying a Security Policy on page 27
3. Deleting a Security Policy on page 28
4. Searching for a Security Policy on page 28

### Viewing the Details of a Security Policy

1. From the **Security Design** task ribbon, select **Security Whiteboard > Security Policy**. The **Manage Policies** inventory panel is displayed.
2. Double-click the icon for the security policy whose details you intend to view. The details of the security policy are displayed in the **Security Policy Details** window.
3. Click **Close**.

### Modifying a Security Policy

To modify a security policy you have created, perform the following steps:

1. From the **Security Design** task ribbon, select **Security Whiteboard > Security Policy**. The **Manage Policies** inventory panel is displayed.
2. Right-click the security policy which you want to modify and select **Modify Policy** from the contextual menu. The **Modify Policy** window is displayed. 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 choose to modify a security policy using the **Actions Panel**. To do so:

1. Select the check box on the left corner of the security policy you want to modify.
2. Click the **Actions Panel** located on the left corner of the inventory panel and select **Modify Policy**.
3. Make necessary changes and click **Modify** to save the changes.

## Deleting a Security Policy

To delete a security policy you have created, perform the following steps:

1. From the **Security Design** task ribbon, select **Security Whiteboard > Security policy**. The **Manage Policies** inventory panel is displayed.
2. Right-click the security policy which you want to delete and select **Delete Policy** from the contextual menu. The **Delete Policy** window is displayed.
3. Select the security policy you want to delete and click **Delete**.



**NOTE:** You can also choose to delete a security policy using the **Actions Panel**. To do so:

1. Select the check box on the left corner of the security policy you want to delete.
  2. Click the **Actions Panel** located on the left corner of the inventory panel and select **Delete Policy**.
  3. Select the security policy you want to delete and click **Delete**.
- 

## Searching for a Security Policy

To search for a security policy you have created, perform the following steps:

1. From the **Security Design** task ribbon, select **Security Whiteboard > Security Policy**. The **Manage Policies** inventory panel is displayed.
2. Enter the name of security policy you want to search, in the **Search** field.
3. Click the magnifying glass icon next to **Search** field. The **Manage Policies** inventory panel is populated with the security policies matching your search criterion.

- Related Topics**
- Security Policies Overview on page 21
  - Creating Security Policies on page 22
  - Deploying Security Policies on page 28

## Deploying Security Policies

---

To deploy or provision a security policy you have created, perform the following steps:

1. From the **Security Design** task ribbon, select **Security Whiteboard > Security policy**. The **Manage Policies** inventory panel is displayed.
2. Right-click the security policy which you want to provision and select **Provision Policy** from the contextual menu. The next screen displays the devices on which this policy can be provisioned.

3. Select the check box next to the device on which you want to provision this security policy.



NOTE: If you want to view the details of the security policy, click the “+” symbol next to the device on which you want to provision the security policy. Click the **Rules** tab and view the applications that are a part of the security domains and their actions and directions.

4. Select the check box next to the **Schedule Provisioning** field to schedule the provisioning to a later time and date. Click **Next**.
5. Select appropriate values from the **Date and Time** field.
6. Click **Provision** on the following window. The security policy is provisioned on the device/s you have chosen.



NOTE: You can also provision the policy from the Policy Designer Whiteboard. To do so right-click the line between security domains and select **Provision Policy** from the contextual menu. Perform steps 3 through 6 to provision the security policy.

#### Related Topics

- Security Policies Overview on page 21
- Creating Security Policies on page 22
- Managing Security Policies on page 27



## CHAPTER 5

# VPN Proposals

- VPN Proposals Overview on page 31
- Creating VPN Proposals on page 32
- Managing VPN Proposals on page 36

### VPN Proposals Overview

You can use a VPN Proposal Wizard to create an object that specifies the IKE and IPsec proposals used in an IPsec VPN. An IKE proposal authenticates peers and negotiates IPsec parameters to establish IPsec SAs. IPsec proposal exchanges information between established IPsec SAs through an IPsec tunnel.

Junos Space allows you to configure the following parameters for a VPN proposal:

- Diffie-Hellman group used by the IKE and IPsec proposal
- Authentication algorithm used by the IKE and IPsec proposal – MD5, SHA, SHA 2
- Encryption standard used by the IKE and IPsec proposal – DES, 3DES, AES
- Life time of the IKE and IPsec proposal
- Life size for the IPsec proposal

When a VPN proposal is created, Junos Space creates an object in the Junos Space database to represent the VPN proposal. This object can be used to create VPN profiles.

Junos Space provides three Juniper Networks defined VPN proposals. The parameters of these VPN proposals are shown in Table 4 on page 31.

**Table 4: Default VPN Proposals**

Proposal Name	Authentication Algorithm	Encryption Standard	Key Exchange
High Security	SHA	AES	DH Group 2 and ESP Protocol
Medium Security	SHA/MD5	3DES	DH Group 2 / Group 1 and ESP Protocol
Low Security	MD5	DES	DH Group 1 and AH Protocol



NOTE: You cannot modify or delete Juniper Networks defined VPN proposals. You can only copy them and create new VPN proposals.

- Related Topics**
- Creating VPN Proposals on page 32
  - Managing VPN Proposals on page 36

## Creating VPN Proposals

To create a new VPN proposal, perform the following steps:

1. From the **Security Design** task ribbon, select **Security Whiteboard > IPSec VPN > VPN Proposal**. The **Manage VPN Proposals** inventory panel is displayed with the icons for all the VPN proposals as shown in Figure 12 on page 32. The first three proposals listed here are Juniper Networks defined VPN proposals.

Figure 12: Manage VPN Proposals Inventory Panel



2. From the task ribbon, select the **Create VPN Proposal** icon. The **Create VPN Proposal** window is displayed as shown in Figure 13 on page 33.



Figure 13: Create VPN Proposal Window

3. In the **Name** field, enter a name for the new VPN proposal.
4. In the **Description** field, enter a description for the new VPN proposal.
5. In the **IKE Proposals** panel, click the **Add** icon. The **IKE Proposal** dialog box is displayed.
6. You can either add a predefined proposal or a custom proposal in the **IKE Proposal** dialog box. To add a predefined IKE proposal:
  - a. Select the **Predefined** check box.
  - b. From the **Name** field, select an appropriate proposal
7. To add a custom IKE proposal:

- a. Select the **Custom** check box as shown in Figure 14 on page 34.

Figure 14: Adding a Custom IKE Proposal

The screenshot shows the 'IKE Proposal' dialog box. At the top, there are two radio buttons: 'Predefined' and 'Custom'. The 'Custom' radio button is selected. Below the radio buttons, there are five input fields: 'Name' (a text box), 'DH Group' (a dropdown menu showing 'Please select ...'), 'Authentication' (a dropdown menu showing 'SHA-1'), 'Encryption' (a dropdown menu showing '3DES'), and 'Life Time (in seconds)' (a text box showing '3600'). At the bottom of the dialog, there are three buttons: 'Restore Defaults', 'Add', and 'Cancel'.

- b. In the **Name** field, enter an appropriate name for the custom proposal.
- c. From the **DH Group** field, select an appropriate group
- d. From the **Authentication** field, select an appropriate authentication algorithm.
- e. From the **Encryption** field, select an appropriate encryption standard.
- f. In the **Life Time (in seconds)** field, enter a value in seconds. The default value of the lifetime is 3600 seconds.



**NOTE:** IKE lifetime defines the duration of an IKE connection. When this time expires, a new phase -1 exchange is performed.

8. Click **Restore Defaults** to restore the default settings.
9. Click **Add** to add the proposal. Repeat Steps 5 to 9 to add a maximum of four proposals. The proposal/s you have added is/are displayed in the **IKE Proposals** panel.
10. In the **IPSec Proposals** panel, click the **Add** icon. The **IPSec Proposal** dialog box is displayed.
11. You can either add a predefined proposal or a custom Proposal, in the **IPSec Proposal** dialog box. To add a predefined IPSec proposal:
  - a. Select the **Predefined** check box.
  - b. From the **Name** field, select an appropriate proposal.
12. To add a custom IPSec proposal:

- a. Select the **Custom** check box as shown in Figure 15 on page 35.

Figure 15: Adding a Custom IPsec Proposal

The screenshot shows the 'IPsec Proposal' dialog box. At the top, there are two radio buttons: 'Predefined' and 'Custom'. The 'Custom' radio button is selected. Below the radio buttons, there are several input fields and dropdown menus: 'Name' (text input), 'DH Group' (dropdown menu with 'Please select ...'), 'Authentication' (dropdown menu with 'SHA-1'), 'Protocol' (dropdown menu with 'Please select ...'), 'Encryption' (dropdown menu with '3DES'), 'Life Time (in seconds)' (text input with '28800'), and 'Life Size (in KBs)' (text input). At the bottom of the dialog, there are three buttons: 'Restore Defaults', 'Add', and 'Cancel'.

- b. In the **Name** field, enter an appropriate name for the custom proposal.
- c. From the **DH Group** field, select an appropriate group.
- d. From the **Authentication** field, select an appropriate authentication algorithm.
- e. From the **Encryption** field, select an appropriate encryption standard.
- f. In the **Life Time (in seconds)** field, enter a value in seconds. The lifetime values for an IPsec proposal can range between 180 to 86,400 seconds.
- g. In the **Life Size (in KBs)** field, enter a value in Kilo Bytes. The lifesize values for an IPsec proposal can range between 64 to 1048576 Kilo Bytes.



**NOTE:** IPsec lifetime defines the duration of a VPN connection. When either of the lifetime or lifesize value expires, a re-key is initiated with a new IPsec encryption and authentication session keys.

13. Click **Add** to add the proposal. Repeat Steps 10 to 13 to add a maximum of four proposals. The proposal/s you have added is/are displayed in the **IPsec Proposals** panel.
14. Click **Create** to create a VPN proposal. The new proposal you have created is displayed in the **Manage VPN Proposals** inventory panel.

- Related Topics**
- VPN Proposals Overview on page 31
  - Managing VPN Proposals on page 36

## Managing VPN Proposals

---

You can view, delete, modify or copy proposals listed in the **Manage VPN Proposals** inventory panel. To open the **Manage VPN Proposals** inventory panel:

- From the **Security Design** task ribbon, select **Security Whiteboard > IPSec VPN > VPN Proposal**. The **Manage VPN Proposals** inventory panel is displayed. All VPN proposals created so far is listed by default, in the graphical view.

The tasks that can be performed in the **Manage VPN Proposals** space include:

1. Viewing the Details of a VPN Proposal on page 36
2. Modifying a VPN Proposal on page 37
3. Deleting a VPN Proposal on page 38
4. Copying a VPN Proposal on page 39
5. Searching for a VPN Proposal on page 39

### Viewing the Details of a VPN Proposal

To view the details of a VPN proposal, perform the following steps:

1. From the **Security Design** task ribbon, select **Security Whiteboard > IPSec VPN > VPN Proposal**. The **Manage VPN Proposals** inventory panel is displayed.
2. Double-click the icon for the VPN proposal whose details you intend to view. The details of the proposal are displayed in the **VPN Profile** details window as shown in Figure 16 on page 37. The **VPN Profile Details** window lists all the IKE and IPSec proposals used in this VPN proposal.

Figure 16: Viewing VPN Proposal Details

**VPN Proposal Details**

Name: VPN\_Proposal1

Definition Type: Custom

Description:

IKE Proposals					
Name	Type	DH Group	Auth Algorithm	Encryption Algorithm	Life Time (in secs)
g2-3des-sha1	Predefined	Group2	SHA-1	3DES	28800
g5-aes256-sha1	Predefined	Group5	SHA-2(256)	AES(256)	28800
High_security	Custom	Group2	SHA-1	3DES	3600

IPSec Proposals							
Name	Type	DH Group	Auth Algorithm	Encryption Algorithm	Life Time (in secs)	Protocol	Life Size (in Bytes)
g5-esp-aes128-sha1	Predefined	Group5	SHA-1	AES(128)	3600	ESP	0

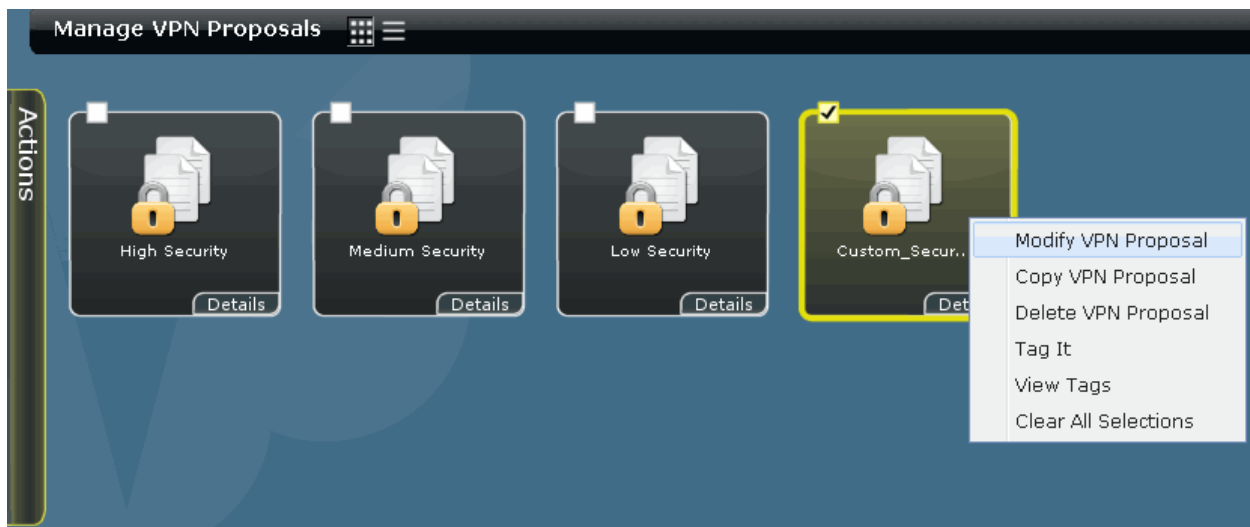
Close

## Modifying a VPN Proposal

To modify a VPN proposal you have created, perform the following steps:

1. From the **Security Design** task ribbon, select **Security Whiteboard > IPSec VPN > VPN Proposal**. The **Manage VPN Proposals** inventory panel is displayed.
2. Right-click the VPN proposal you want to modify and click the **Modify VPN Proposal** link from the contextual menu as shown in Figure 17 on page 38. This action re-directs you to the window that you used to create a new VPN proposal. You can modify all the fields on this window, except the **Name** field.

Figure 17: Modifying a VPN Proposal



3. Enter a new description in the **Description** field.
4. To edit an IKE or IPSec proposal, select the proposal you want to edit and click the **Edit** icon in the corresponding panel. The corresponding dialog box is displayed.
5. Make necessary changes to your IKE or IPSec proposal and click **Modify**.
6. To delete an IKE or IPSec proposal, select the proposal you want to delete in the corresponding panel and click the **Delete** icon. The **Delete Proposal** confirmation window is displayed.
7. Click **Delete**.
8. Click **Modify** to save the changes made to this VPN proposal.



**NOTE:** You can also choose to modify a VPN proposal using the Actions Panel. To do so:

1. Select the check box on the left corner of the VPN proposal you want to modify.
2. Click the **Actions Panel** located on the left corner of the inventory panel and select **Modify VPN Proposal**.
3. Make necessary changes and click **Modify** to save the changes.

## Deleting a VPN Proposal

To delete a VPN proposal you have created, perform the following steps:

1. From the **Security Design** task ribbon, select **Security Whiteboard > IPSec VPN > VPN Proposal**. The **Manage VPN Proposals** inventory panel is displayed.

2. Right-click the VPN proposal you intend to delete and click the **Delete VPN Proposal** link from the contextual menu. The **Delete Proposal** confirmation window is displayed.
3. Select the VPN proposal you want to delete and click **Delete**.



NOTE: You can also choose to delete a VPN proposal using the **Actions Panel**. To do so:

1. Select the check box on the left corner of the VPN proposal you want to delete.
2. Click the **Actions Panel** located on the left corner of the inventory panel and select **Delete VPN Proposal**.
3. Select the VPN proposal you want to delete and click **Delete**.



NOTE: You cannot delete a VPN proposal that is already used in a VPN profile. To delete a VPN proposal that is a part of a VPN proposal, you should first dis-associate the VPN proposal from the VPN profile.

## Copying a VPN Proposal

To copy a VPN proposal you have created, perform the following steps:

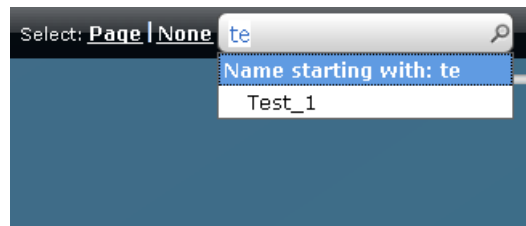
1. From the **Security Design** task ribbon, select **Security Whiteboard > IPSec VPN > VPN Proposal**. The **Manage VPN Proposals** inventory panel is displayed.
2. Select a VPN proposal you want to copy and click the **Copy Proposal** link from the **Actions** panel located on the left corner of the inventory panel. This action re-directs you to the window that you used to create a new VPN proposal. This window displays the parameters of the proposal you have copied with the **Name** field left blank.
3. In the **Name** field, enter a name for the new VPN proposal.
4. Edit the other fields of the proposal if you intend to do so.
5. Click **Create** to create a new proposal. The new proposal you have created is displayed in the **Manage VPN Proposals** Inventory panel.

## Searching for a VPN Proposal

To search for a VPN proposal you have created, perform the following steps:

1. From the **Security Design** task ribbon, select **Security Whiteboard > IPSec VPN > VPN Proposal**. The **Manage VPN Proposals** inventory panel is displayed.
2. Enter the name of VPN proposal you want to search, in the **Search** field as shown in Figure 18 on page 40.

Figure 18: Searching for a VPN Proposal



3. Click the magnifying glass icon next to **Search** field. The **Manage VPN Proposals** inventory panel is populated with the VPN proposals matching your search criterion.

- Related Topics**
- VPN Proposals Overview on page 31
  - Creating VPN Proposals on page 32



## CHAPTER 6

# VPN Profiles

- [VPN Profiles Overview on page 41](#)
- [Creating VPN Profiles on page 42](#)
- [Managing VPN Profiles on page 48](#)

### VPN Profiles Overview

---

You can use a VPN Profile Wizard to create an object that specifies the VPN proposals, IKE/IPSec settings and the connectivity parameters used in a route-based IPSec VPN.

Junos Space allows you to configure the following parameters for a VPN profile:

- VPN Proposals – predefined or custom proposals created using the VPN Proposal Wizard
- IKE Settings – Authentication mode, Pre-shared key authentication mode, NAT Reversal, and Dead Peer Detection
- IPSec Settings – Proxy ID, Idle Time, Install Interval, Anti Replay, and VPN Monitor
- Tunnel Interface Settings – Interface type, and Interface zone

When a VPN profile is created, Junos Space creates an object in the Junos Space database to represent the VPN profile. This object can be used to create route-based IPSec VPNs.

Junos Space provides two Juniper Networks defined VPN profiles:

- Site-To-Site – used between peers using static IP addresses. It uses Preshared Key based authentication, High Security VPN proposal, Unnumbered tunnel interface and default values for other parameters.
- Hub-Spoke – used when one of the peers has a dynamic IP address. It uses Preshared Key based authentication, High Security VPN proposal, Unnumbered tunnel interface and default values for other parameters.



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

---

**Related Topics** • [Creating VPN Profiles on page 42](#)

- Managing VPN Profiles on page 48

## Creating VPN Profiles

To create a new VPN Profile, perform the following steps:

1. From the **Security Design** task ribbon, select **Security Whiteboard > IPSec VPN > VPN Profile**. The **Manage VPN Profiles** inventory panel is displayed with the icons for all the VPN profiles as shown in Figure 19 on page 42. The first two profiles listed here are Juniper Networks defined VPN profiles.

Figure 19: Default VPN Profiles



2. From the task ribbon, select the **Create VPN Profile** icon. The **General** panel of the **Create VPN Profile** window is displayed as shown in the Figure 20 on page 43.

Figure 20: Creating a VPN Profile

**General**

**General**

Name:

Type: Route Based

Description:

**VPN Proposal**

Proposal Type: ☒ Predefined ☐ Custom

Predefined Proposals:

High Medium Low

Back Next Finish Cancel

Creating a VPN profile involves the following tasks:

- Specifying the general settings
- Specifying the IKE/IPSec settings
- Specifying the connectivity parameters

### Specifying the general settings

To specify the general settings for the VPN profile:

1. In the **General** Section:
  - a. In the **Name** field, enter a name for the new VPN profile.
  - b. In the **Description** field, enter a description for the new VPN profile.
2. In the **VPN Proposal** section:
  - a. Choose a proposal you intend to use. To choose one of the Juniper Networks defined proposals, select the **Predefined** radio button.
  - b. Drag the slider to the intended position on the **Predefined Proposals** slider bar. You can choose to place the slider at the **High**, **Medium** or **Low** markers to choose the associated proposals, as shown in the Figure 21 on page 44. Mouse over on 'High', 'Medium' and 'Low' text to get a tool tip description about the respective predefined proposal.

Figure 21: Choosing a Default VPN Proposal

The screenshot shows the "VPN Proposal" configuration window. At the top, "Proposal Type" has two radio buttons: "Predefined" (selected) and "Custom". Below this is a "Predefined Proposals" slider with three positions: "High", "Medium", and "Low". The slider is currently positioned at "Medium". A tooltip box is displayed over the "Medium" position, containing the text: "Juniper defined Medium Security VPN Proposal. It uses 3DES encryption, SHA authentication, DH Group 2 Key exchange and ESP protocol." At the bottom of the window are four buttons: "Back", "Next", "Finish", and "Cancel".

- c. To choose a custom VPN proposal you have created using the Create VPN Proposal Wizard, select the **Custom** radio button. The **VPN Proposal** section refreshes. You can choose a custom VPN proposal or create new VPN proposals.
- d. From the **Custom Proposals** drop-down menu, choose a custom VPN proposal that you have already created and stored, as shown in Figure 22 on page 44.

Figure 22: Choosing a Custom VPN Proposal

The screenshot shows the "VPN Proposal" configuration window. At the top, "Proposal Type" has two radio buttons: "Predefined" and "Custom" (selected). Below this is a "Custom Proposals" section with a text input field and a dropdown arrow. To the right of this field is a button labeled "Add New Proposal".

- e. If you want to add a new VPN proposal, click **Add New Proposal**. This re-directs you to the VPN Proposal creation page. For more information on creating a VPN proposal, see "Creating VPN Proposals" on page 32.
3. Click **Next** to continue. The **IKE/IPSec Setting** panel of the **Create VPN Profile** window is displayed.

### Specifying the IKE/IPSec settings

To specify the IKE settings in the **IKE Settings** section:

1. Select the **Main** radio button or the **Aggressive** radio button to select the mode of authentication, as shown in Figure 23 on page 45.

Figure 23: Specifying IKE Settings

**IKE/IPSec Settings**

**IKE Settings**

Mode: ☒ Main ☐ Aggressive

IKE Identity:

Authentication: Preshared Key

Preshared Key: ☐ Auto Generate ☒ Manual

Key Phrase:

**Advanced IKE Settings**

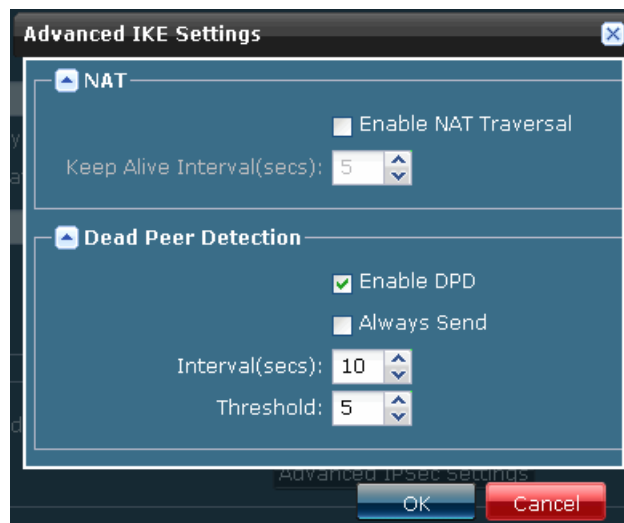
**IPSec Settings**

☐ Use Proxy Id

**Advanced IPSec Settings**

2. From the **IKE Identity** drop-down menu, select an appropriate mode to identify IKE peers.
3. Select how the pre-shared key is generated by choosing appropriate the radio button.
  - a. Select the **Auto Generate** radio button to auto-generate the pre-shared key.
  - b. Select the **Manual** radio button to specify a pre-shared key manually.
  - c. Enter the pre-shared key in the **Key Phrase** field.
4. To configure advanced IKE settings, click **Advanced IKE Settings**. The **Advanced IKE Settings** dialog box is displayed, as shown in Figure 24 on page 46.

Figure 24: Specifying Advanced IKE Settings

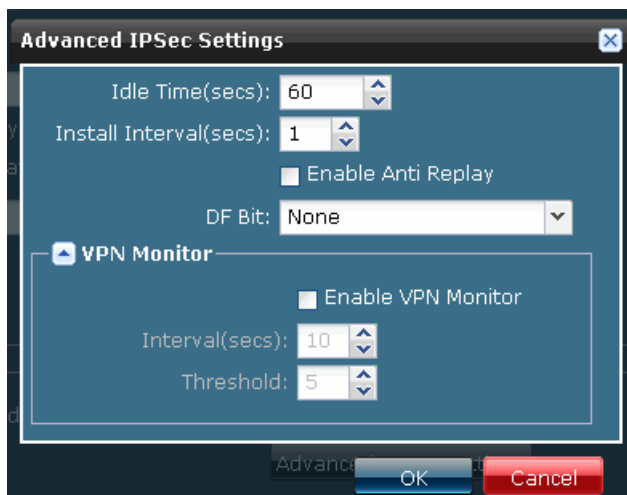


5. In the **NAT** section:
  - a. Select/Clear the **Enable NAT Traversal** check box to enable/disable the NAT traversal feature respectively.
  - b. In the **Keep Alive Interval (secs)** field, enter a value in seconds. You can also increase or decrease the value currently displayed by selecting the upward or downward pointing arrows respectively.
6. In the **Dead Peer Detection** section:
  - a. Select/Clear the **Enable DPD** check box to enable/disable the Dead Peer Detection feature respectively.
  - b. Select/Clear the **Always Send** check box to enable/disable the Always Send feature respectively.
  - c. In the **Interval (secs)** field, enter a value in seconds. You can also increase or decrease the value currently displayed by selecting the upward or downward pointing arrows respectively.
  - d. In the **Threshold** field, enter a value. You can also increase or decrease the value currently displayed by selecting the upward or downward pointing arrows respectively.
7. Click **OK** to save these settings.

To specify the IPSec settings in the **IPSec Settings** section:

1. Select/Clear the **Use Proxy ID** check box to enable/disable the Proxy ID feature respectively.
2. To configure advanced IPSec settings, click **Advanced IPSec Settings**. The **Advanced IPSec Settings** dialog box is displayed, as shown in Figure 25 on page 47.

Figure 25: Specifying Advanced IPsec Settings



3. In the **Idle Time (secs)** field, enter a value in seconds. You can also increase or decrease the value currently displayed by selecting the upward or downward pointing arrows respectively.
4. In the **Install Interval (secs)** field, enter a value in seconds. You can also increase or decrease the value currently displayed by selecting the upward or downward pointing arrows respectively.
5. Select/Clear the **Enable Anti Replay** check box to enable/disable the Anti Replay feature respectively.
6. Select an appropriate option from the **DF Bit** field. This option specifies if a router is allowed to fragment a packet.
7. Select/Clear the **Enable VPN Monitor** check box to enable/disable the Enable VPN Monitor feature respectively. Configure the following options in the **VPN Monitor** section.
  - a. In the **Interval (secs)** field, enter a value in seconds. You can also increase or decrease the value currently displayed by selecting the upward or downward pointing arrows respectively.
  - b. In the **Threshold** field, enter a value. You can also increase or decrease the value currently displayed by selecting the upward or downward pointing arrows respectively.
8. Click **OK** to save these settings.
9. Click **Next** to continue. The **Connectivity Parameters** panel of the **Create VPN Profile** window is displayed.

### Specifying the connectivity parameters

To specify the connection parameters in the Connectivity Parameters Panel:

1. In the **Tunnel Interface Settings** section:

- a. From the **Interface Type** drop-down menu, select whether the interface is numbered or unnumbered, as shown in Figure 26 on page 48.

**Figure 26: Specifying Connectivity Parameters**

The screenshot shows a window titled "Connectivity Parameters" with a section titled "Tunnel Interface Settings". Inside this section, there are four fields: "Tunnel Interface" set to "Auto Pick", "Interface Type" set to "Unnumbered" with a dropdown arrow, "Interface Zone" set to "vpn", and a checked checkbox labeled "Enable Multipoint".

- b. In the **Interface Zone** section, enter the name for the interface zone.
  - c. Select/Clear the **Enable Multipoint** check box to specify if you want to enable/disable a multipoint interface for this VPN profile.
2. Click **Finish** to save the VPN profile.

- Related Topics**
- VPN Profiles Overview on page 41
  - Managing VPN Profiles on page 48

## Managing VPN Profiles

You can view, delete, modify, or copy VPN profiles listed in the **Manage VPN Profiles** inventory panel. To open the **Manage VPN Profiles** inventory panel:

- From the **Security Design** task ribbon, select **Security Whiteboard > IPSec VPN > VPN Profile**. The **Manage VPN Profiles** inventory panel is displayed. All VPN profiles created are listed by default, in the graphical view.

The tasks that can be performed in the **Manage VPN Profiles** space include:

1. Viewing the Details of a VPN Profile on page 48
2. Modifying a VPN Profile on page 49
3. Deleting a VPN Profile on page 50
4. Copying a VPN Profile on page 51
5. Searching for a VPN Profile on page 51

### Viewing the Details of a VPN Profile

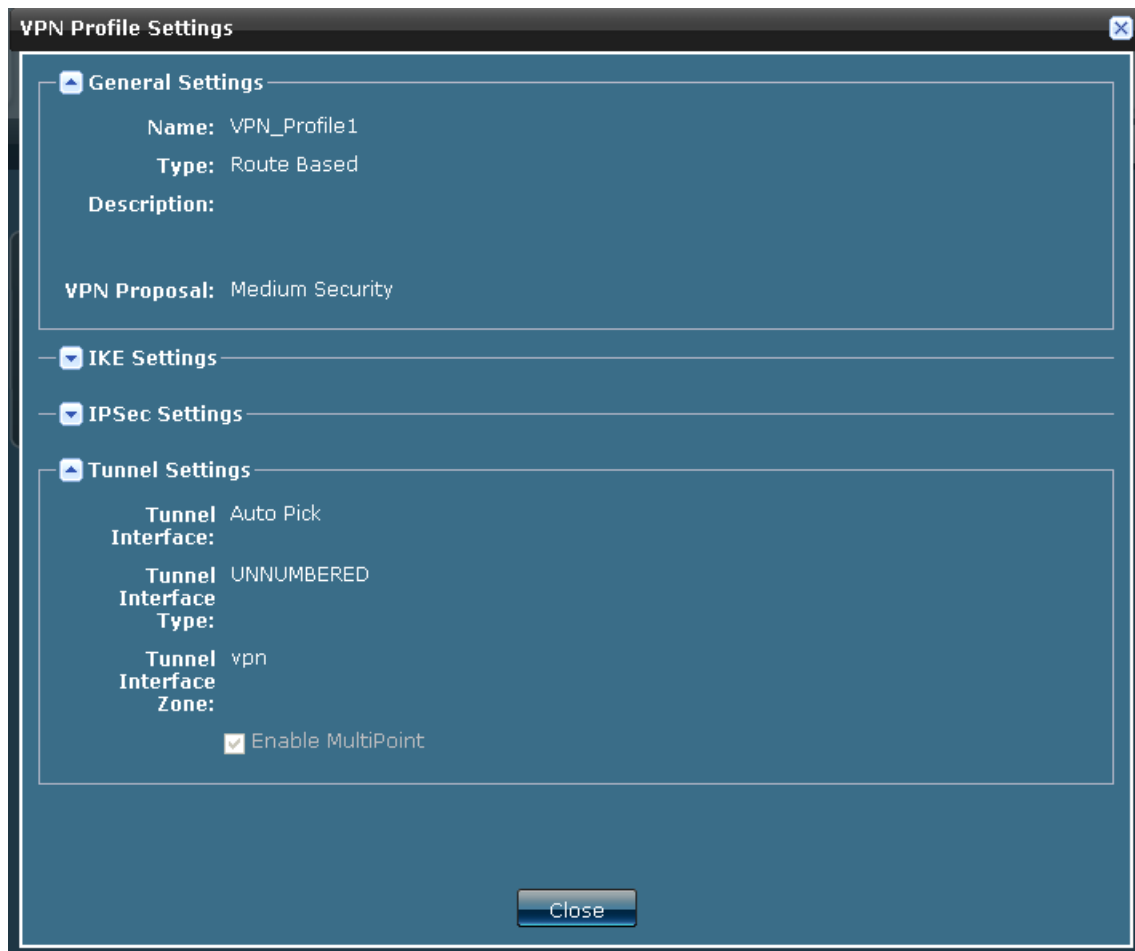
To view the details of a VPN profile, perform the following steps:

1. From the **Security Design** task ribbon, select **Security Whiteboard > IPSec VPN > VPN Profile**. The **Manage VPN Profiles** inventory panel is displayed.
2. Double-click the icon for the VPN profile whose details you intend to view. The details of the VPN profile are displayed in the **VPN Profile Settings** window as shown in



Figure 27 on page 49. The **VPN Profile Settings** window lists all the parameters you have specified for this profile.

Figure 27: Viewing the Details of a VPN Profile



## Modifying a VPN Profile

To modify a VPN profile you have created, perform the following steps:

1. From the **Security Design** task ribbon, select **Security Whiteboard > IPsec VPN > VPN Profile**. The **Manage VPN Profiles** inventory panel is displayed.
2. Right-click the VPN profile and click the **Modify VPN Profile** link from the contextual menu, as shown in Figure 28 on page 50. This action re-directs you to the window that you used to create a new VPN profile. You can modify all the fields in this window, except the **Name** field.

Figure 28: Modifying a VPN Profile



3. Enter a new description in the **Description** field.
4. Make necessary changes to the fields in the **VPN Proposal** section.
5. Click **Next**.
6. Make necessary changes to the fields in the **IKE Settings** and **IPSec Settings** sections in the **IKE/IPSec Settings** Panel.
7. Click **Next**.
8. Make necessary changes to the fields in the **Tunnel Interface Settings** and **Policy Settings** sections in the **Connectivity Parameters** panel.
9. Click **Finish** to save the changes.



NOTE: You can also choose to modify a VPN profile using the **Actions Panel**. To do so:

1. Select the check box on the left corner of the VPN profile you want to modify.
2. Click the **Actions Panel** located on the left corner of the inventory panel and select **Modify VPN Profile**.
3. Make necessary changes and click **Modify** to save the changes.

## Deleting a VPN Profile

To delete a VPN profile you have created, perform the following steps:

1. From the **Security Design** task ribbon, select **Security Whiteboard > IPSec VPN > VPN Profile**. The **Manage VPN Profiles** inventory panel is displayed.
2. Right-click the VPN profile you intend to delete and click the **Delete VPN Profile** link from the contextual menu. The **Delete Profile** confirmation window is displayed.

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



NOTE: You can also choose to delete a VPN profile using the **Actions Panel**. To do so:

1. Select the check box on the left corner of the VPN profile you want to delete.
2. Click the **Actions Panel** located on the left corner of the inventory panel and select **Delete VPN Profile**.
3. Select the VPN profile you want to delete and click **Delete**.

## Copying a VPN Profile

To copy a VPN profile you have created, perform the following steps:

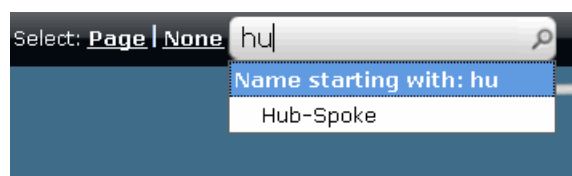
1. From the **Security Design** task ribbon, select **Security Whiteboard > IPSec VPN > VPN Profile**. The **Manage VPN Profiles** inventory panel is displayed.
2. Select a VPN profile you want to copy and click the **Copy VPN Profile** link from the **Actions** panel located on the left corner of the inventory panel. This action re-directs you to the window that you used to create a new VPN profile. This window displays the parameters of the profile you have copied with the **Name** field left blank.
3. In the **Name** field, enter a name for the new VPN profile.
4. Edit the other fields in the **General** panel if you intend to do so.
5. Click **Next**.
6. Edit the fields in the **IKE/IPSec Settings** panel if you intend to do so.
7. Click **Next**.
8. Edit the fields in the **Connectivity Parameters** panel if you intend to do so.
9. Click **Finish** to create a new profile. The new profile you have created is displayed in the **Manage VPN Profiles** inventory panel.

## Searching for a VPN Profile

To search for a VPN profile you have created, perform the following steps:

1. From the **Security Design** task ribbon, select **Security Whiteboard > IPSec VPN > VPN Profile**. The **Manage VPN Profiles** inventory panel is displayed.
2. Enter the name of VPN profile you want to search, in the **Search** field as shown in Figure 29 on page 51.

Figure 29: Searching for a VPN Profile



3. Click the magnifying glass icon next to **Search** field. The **Manage VPN Profiles** inventory panel is populated with the VPN profiles matching your search criterion.

- Related Topics**
- VPN Profiles Overview on page 41
  - Creating VPN Profiles on page 42

## CHAPTER 7

# IPSec VPN

- [IPSec VPNs Overview on page 53](#)
- [Creating IPSec VPNs on page 53](#)
- [Managing IPSec VPNs on page 57](#)
- [Deploying IPSec VPNs on page 59](#)

### IPSec VPNs Overview

---

You can use an IPSec VPN Creation Wizard to create Site-To-Site and Hub-And-Spoke VPNs. The security topology created using the Topology Designer serves as a base to create an IPSec VPN. The following are the prerequisites to configure an IPSec VPN:

- VPN proposal
- VPN profile
- Security topology

You can configure the following parameters for an IPSec VPN:

- Tunnel IP range - in case you want to use a VPN profile with a numbered tunnel interface
- Endpoints for a Site-To-Site VPN
- Spokes and Hubs for a Hub-And-Spoke VPN

The VPN Creation Wizard allows you to view an overlay of the VPN you are creating on your security topology. This helps you make modifications to the VPN design before saving the configuration. Once the configuration is saved you can provision this VPN on the security devices that are a part of this VPN.

#### Related Topics

- [Creating IPSec VPNs on page 53](#)
- [Managing IPSec VPNs on page 57](#)
- [Deploying IPSec VPNs on page 59](#)

### Creating IPSec VPNs

---

To create an IPSec VPN, perform the following steps:

- From the **Security Design** task ribbon, select **Security Whiteboard** > **IPSec VPN**. The **Manage VPNs** inventory panel is displayed. All IPSec VPNs created are listed by default, in the graphical view.
- From the task ribbon, select the **Create IPSec VPN** icon. The **General** panel of the **Create IPSec VPN** window is displayed as shown in Figure 30 on page 54.

Figure 30: Create IPSec VPN:General Panel

The screenshot shows the 'General' panel of the 'Create IPSec VPN' window. It has a dark blue background. At the top, there's a 'Name:' label followed by a text input field. Below that is a 'Description:' label followed by a larger text input field. The 'VPN Type:' label is followed by two icons: 'Site To Site' (a padlock with a green line) and 'Hub And Spoke' (a padlock with a green star). The 'Site To Site' icon is highlighted with a blue border. Below the icons is a 'Select Profile:' label followed by a dropdown menu. The dropdown menu is open, showing two options: 'Site-To-Site' (highlighted with a yellow border) and 'Hub-Spoke'. At the bottom right, there are four buttons: 'Back' (disabled), 'Next' (active), 'Finish' (disabled), and 'Cancel' (red).

1. In the **Name** field, enter a name for the new Site-To-Site VPN.
2. In the **Description** field, enter a description for the new Site-To-Site VPN.
3. From the **VPN Type** field, choose the VPN type you want to create.
4. From the **Select Profile** field, choose an appropriate VPN profile.
5. If you have chosen a VPN profile which has a numbered tunnel interface, the **Tunnel IP Range** fields are displayed. Enter an appropriate tunnel IP range.



NOTE: You should enter a tunnel IP range that is unique for this VPN. You will not be able to use this IP range for other VPNs that are created in the future.

6. Click **Next**. This screen displays your security topology you have created using the Topology Designer. You can create a Site-To-Site or a Hub-And-Spoke VPN based on the VPN type you have chosen in the **VPN Type** field.



NOTE: If you select **Site-To-Site** as the VPN type, only those VPN profiles which use the Main mode to negotiate keys are available for selection. The VPN profiles which use Aggressive mode for negotiating keys are not available for selection.



NOTE: If you select **Hub-And-Spoke** as the VPN type, only those VPN profiles which use a numbered tunnel interface are available for selection. The VPN profiles which use an unnumbered tunnel interface are not available for selection.

1. Site-To-Site on page 55
2. Hub-And-Spoke on page 56

## Site-To-Site

To create a Site-To-Site IPSec VPN, perform the following steps:

1. Right-click the device or the network that is the first endpoint of the VPN and select **Mark Endpoint** from the contextual menu. The device or network chosen as an endpoint displays an overlay icon.



NOTE: If you right-click a network and mark it as an endpoint, the device associated with the network is selected as an endpoint by default.



NOTE: If you right-click a device and mark it as an endpoint, all networks associated with the device is a part of the endpoint.



NOTE: You cannot configure a device group as an endpoint for a Site-To-Site VPN.



NOTE: You cannot select a network that is associated with multiple devices as an endpoint for a Site-To-Site VPN.

2. Right-click the device or the network that is the second endpoint of the VPN and select **Mark Endpoint** from the contextual menu.

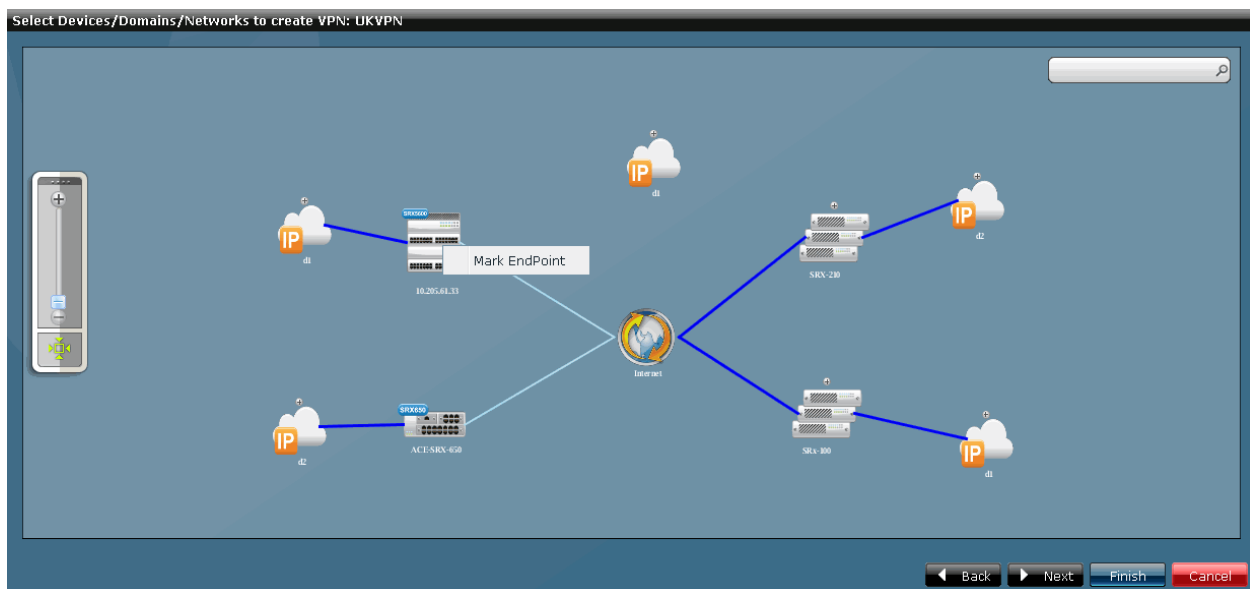
3. Click **Next**. This screen displays an overlay of the VPN you are creating over the topology design. You can also view the tunnels that connect the endpoints.
4. Click **Finish** to complete the VPN creation. The new VPN you have created is displayed in the **Manage VPNs** inventory panel.

## Hub-And-Spoke

To create a Hub-And-Spoke IPSec VPN, perform the following steps:

1. Right-click the device or the network that is the first spoke of the VPN and select **Mark Endpoint** from the contextual menu, as shown in Figure 31 on page 56.

Figure 31: Marking Endpoints For a VPN



**NOTE:** If you right-click a network and mark it as an endpoint, the device associated with the network is selected as an spoke by default.



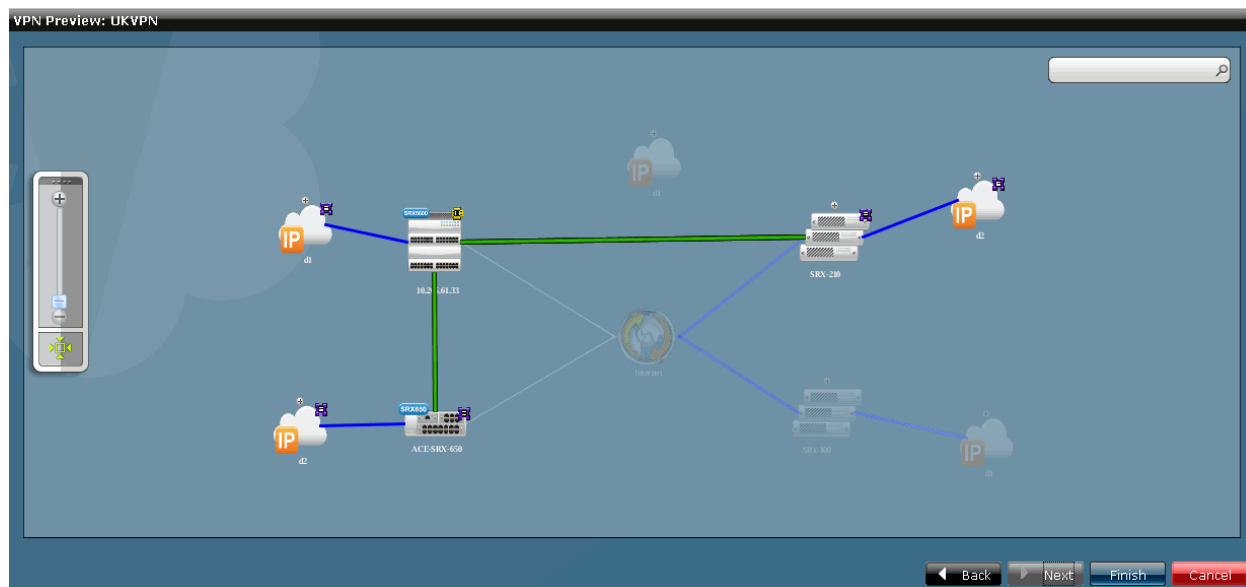
**NOTE:** If you right-click a device and mark it as an endpoint, all networks associated with the device is a part of the spoke.

2. Right-click the device or the network that is the second spoke of the VPN and select **Mark Endpoint** from the contextual menu.
3. Right-click the device or the network that is the third spoke of the VPN and select **Mark Endpoint** from the contextual menu.
4. Right-click the spoke that you intend to configure as a hub and select **Mark Hub** from the contextual menu. The overlay icon changes to the one indicating a hub in the VPN.



- Click **Next**. This screen displays an overlay of the VPN you are creating over the topology design. You can also view the tunnels that connect the hub/s with the spokes, as shown in Figure 32 on page 57.

Figure 32: VPN Preview



- Click **Finish** to complete the VPN creation. The new VPN you have created is displayed in the **Manage VPNs** inventory panel.

- Related Topics**
- IPSec VPNs Overview on page 53
  - Managing IPSec VPNs on page 57
  - Deploying IPSec VPNs on page 59

## Managing IPSec VPNs

You can edit or delete the IPSec VPNs listed in the **Manage VPNs** inventory panel. To open the **Manage VPNs** inventory panel:

- From the **Security Design** task ribbon, select **Security Whiteboard** > **IPSec VPN**. The **Manage VPNs** inventory panel is displayed. All IPSec VPNs created so far is listed by default, in the graphical view.

The tasks that can be performed in the **Manage VPNs** space include:

- Modifying a IPSec VPN on page 58
- Deleting an IPSec VPN on page 58

## Modifying a IPSec VPN

To modify an IPSec VPN you have created, perform the following steps:

1. From the **Security Design** task ribbon, select **Security Whiteboard > IPSec VPN**. The **Manage VPNs** inventory panel is displayed.
2. Right-click the IPSec VPN and click the **Modify VPN** link from the contextual menu. This action re-directs you to the window that you used to create a new IPSec VPN. You can modify all the fields on this window, except the **Name** field and the **VPN Type** field.
3. Enter a new description in the **Description** field.
4. Make necessary changes in the **Select Profile** field.
5. Click **Next**.
6. Make necessary changes to VPN setup and click **Next**. This screen displays an overlay of the VPN you have created over the topology design.
7. Click **Finish** to complete the VPN modification.



NOTE: You can also choose to modify an IPSec VPN using the **Actions Panel**. To do so:

1. Select the check box on the left corner of the IPSec VPN you want to modify.
2. Click the **Actions Panel** located on the left corner of the inventory panel and select **Modify VPN**.
3. Make necessary changes and click **Finish** to save the changes.

---

## Deleting an IPSec VPN

To delete an IPSec VPN you have created, perform the following steps:

1. From the **Security Design** task ribbon, select **Security Whiteboard > IPSec VPN**. The **Manage VPNs** inventory panel is displayed.
2. Right-click the IPSec VPN you intend to delete and click the **Delete VPN** link from the contextual menu. The **Delete VPN** confirmation window is displayed.
3. Select the IPSec VPN you want to delete and click **Delete**.



NOTE: You can also choose to delete an IPSec VPN using the **Actions Panel**. To do so:

1. Select the check box on the left corner of the IPSec VPN you want to delete.
  2. Click the **Actions Panel** located on the left corner of the inventory panel and select **Delete VPN**.
  3. Select the IPSec VPN you want to delete and click **Delete**.
-

- Related Topics**
- IPSec VPNs Overview on page 53
  - Creating IPSec VPNs on page 53
  - Deploying IPSec VPNs on page 59

## Deploying IPSec VPNs

To deploy or provision an IPSec VPN you have created, perform the following steps:

1. From the **Security Design** task ribbon, select **Security Whiteboard > IPSec VPN**. The **Manage VPNs** inventory panel is displayed.
2. Right-click the IPSec VPN which you want to provision and select **Provision VPN** from the contextual menu. The **Provision VPN** window displays the devices on which this VPN is provisioned. You can view the device name, device IP, platform, OS version, configuration state, connection status, and the XML commands, as shown in Figure 33 on page 59.

Figure 33: Provision VPN Window



The screenshot shows a window titled "Provision VPN : London\_VPN". Inside is a table with the following data:

Name	Device IP	Platform	OS Version	Configuration	Connection Status	XML Commands
10.205.61.33	10.205.61.33	SRX5600	10.3	New	up	<a href="#">view</a>
ACE-SRX-650	10.204.79.134	SRX650	10.3	New	up	<a href="#">view</a>

The states displayed in the **Configuration** column specify if the configured pushed to the device is new, a modified one, or one that will be removed.

3. If you want to preview the configuration changes pushed to the device, click the **View** link in the **XML Commands** column corresponding to the device, as shown in Figure 32.

Figure 34: Viewing XML Commands

The screenshot shows a web interface titled "VPN configuration for device - 10.205.61.33". Below the title is a tab labeled "Configuration". The main area displays XML configuration commands for a VPN setup. The XML is as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
  <interfaces>
    <interface>
      <name>st0</name>

      <unit operation="create">
        <name>2</name>
        <family>
          <inet/>
        </family>
      </unit>
    </interface>
  </interfaces>
  <routing-options>
    <static>

      <route operation="create">
        <name>2.2.2.2/32</name>
        <next-hop>st0.2</next-hop>
      </route>
    </static>
  </routing-options>
  <security>
    <ike>

      <policy operation="create">
        <name>London_VPN_Site-To-Site_0_0</name>
        <proposals>g5-aes128-sha2</proposals>
        <proposals>g5-aes192-sha2</proposals>
        <proposals>g5-aes256-sha2</proposals>
        <mode>main</mode>
        <pre-shared-key>
```

4. Select the check box next to the **Schedule Provisioning** field to schedule the provisioning to a later time and date. Click **Next**.
5. Select appropriate values from the **Date and Time** field.
6. Click **Provision** in the following window. The IPSec VPN is provisioned on the device/s that are a part of this VPN. A new job is created and the job ID is displayed in the **Job Information** dialog box.
7. Click the job ID to view more information about the job created. This action directs you to the **Job Management** work space.

The **Device Provisioning Status** window is displayed with the status of the IPSec VPN you have provisioned on each device. You will see appropriate error messages in the **Message** column of this window, if the provisioning fails. The error message include:

- Connection Status is not up- this indicates that there is no active connection to the device from Junos Space.
- Managed Status is not In Sync-this indicates that the latest device configuration is not synched with Junos Space.
- Configuration Update Failed–this indicates configuration commit errors. This error message includes the error message sent by the device.



---

NOTE: You can also choose to provision a VPN using the **Actions Panel**. To do so:

1. Select the check box on the left corner of the VPN you want to provision.
  2. Click the **Actions Panel** located on the left corner of the inventory panel and select **Provision VPN**.
  3. Select the device on which the VPN is to be provisioned and click **Provision**.
- 

**Related Topics**

- [IPSec VPNs Overview on page 53](#)
- [Creating IPSec VPNs on page 53](#)
- [Managing IPSec VPNs on page 57](#)



## CHAPTER 8

# Index

- Index on page 65





# Index

## I

IPSec VPNs	
creating.....	53
deleting.....	58
deploying.....	59
overview.....	53

## S

security policies	
creating.....	22
deleting.....	28
deploying.....	28
modifying.....	27
overview.....	21
searching.....	28
viewing the details.....	27
Security Policy Designer.....	22
security policy profiles	
copying.....	19
creating.....	14
deleting.....	19
modifying.....	18
overview.....	13
searching.....	20
viewing the details.....	17
security topology	
adding addresses and security domains using	
CSV import.....	11
associating addresses with security devices.....	8
associating addresses with security	
domains.....	9
connecting security devices.....	7
creating.....	4
creating address groups.....	9
creating device groups.....	9
creating group links on device groups.....	10
deleting.....	5
drag and drop security devices.....	6
editing.....	5
overview.....	3

removing addresses from a security	
domain.....	9
saving.....	5
searching for objects in topology.....	10
Security Whiteboard Overview.....	1

## V

VPN profiles	
copying.....	51
creating.....	42
deleting.....	50
modifying.....	49
overview.....	41
searching.....	51
viewing the details.....	48
VPN proposals	
copying.....	39
creating.....	32
deleting.....	38
modifying.....	37
overview.....	31
searching.....	39
viewing the details.....	36

