



Junos[®] Space

Security Design User Guide

Release

2.0



Published: 2010-11-15

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

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

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

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

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

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

Juniper Networks, the Juniper Networks logo, JUNOS, NetScreen, ScreenOS, and Steel-Belted Radius are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOSe is a trademark of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

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

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

Junos Space Security Design User Guide
Copyright © 2010, Juniper Networks, Inc.
All rights reserved. Printed in USA.

Revision History
November 2010—Junos Space Security Design User Guide, Release 2.0

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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 IS 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 Juniper 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 is in the English language)).

Table of Contents

	About the Documentation	xvii
	Junos Space Documentation and Release Notes	xvii
	Documentation Conventions	xvii
	Documentation Feedback	xviii
	Requesting Technical Support	xviii
	Self-Help Online Tools and Resources	xviii
	Opening a Case with JTAC	xix
Part 1	Security Design Overview	
Chapter 1	Security Design Overview	3
	Security Design Overview	3
Chapter 2	Security Design Dashboard Overview	5
	Security Design Dashboard Overview	5
Chapter 3	Security Design Gadgets Overview	7
	Security Design Gadgets Overview	7
	Devices Used in Security Topology	7
	Object Count	8
	Address Types	9
	Object Usage	9
	Devices in Security Topology	10
	Job Types	10
	State of Jobs Run	11
	Average Execution Time per Completed Job	11
Part 2	Getting Started	
Chapter 4	Getting Started with Security Design	15
	Getting Started with Security Design	15
	Provisioning an IPsec VPN	15
	Provisioning Firewall Policies	16
Part 3	Object Builder	
	Object Builder Overview	17

Chapter 5	Applications and Application Groups	19
	Application and Application Groups Overview	19
	Creating Applications	20
	Managing Applications	23
	Viewing the Details of an Application	24
	Modifying an Application	24
	Deleting an Application	24
	Searching for an Application	25
	Creating Application Groups	25
	Managing Application Groups	27
	Viewing the Details of an Application Group	28
	Modifying an Application Group	28
	Deleting an Application Group	29
	Searching for an Application Group	29
Chapter 6	Security Domains	31
	Security Domains Overview	31
	Creating Security Domains	32
	Managing Security Domains	34
	Viewing the Details of a Security Domain	35
	Modifying a Security Domain	35
	Deleting a Security Domain	36
	Searching for a Security Domain	36
	Viewing Security Domain Hierarchy	36
Chapter 7	Addresses	39
	Addresses Overview	39
	Creating Addresses	40
	Managing Addresses	42
	Viewing the Details of an Address	42
	Modifying an Address	42
	Deleting an Address	44
	Searching for an Address	44
Part 4	Security Whiteboard	
	Security Whiteboard Overview	45
Chapter 8	Security Topology	47
	Security Topology Overview	47
	Creating a Security Topology	49
	Dragging and Dropping Security Devices	51
	Connecting Security Devices	52
	Dragging and Dropping Addresses	53
	Associating Addresses with Security Devices	53
	Creating Device Groups	54
	Moving Ungrouped Devices into a Device Group	54
	Removing Devices from a Device Group	55
	Searching for Devices and Addresses in the Topology	55
	Creating Group Links on Device Groups	56

	Adding Addresses and Security Domains Using CSV Import	56
	Changing Topology Scapes	57
Chapter 9	Security Policies	59
	Security Policy Profiles Overview	59
	Creating Security Policy Profiles	61
	Managing Security Policy Profiles	64
	Viewing the Details of a Security Policy Profile	64
	Modifying a Security Policy Profile	65
	Copying a Security Policy Profile	65
	Deleting a Security Policy Profile	66
	Searching for a Security Policy	66
	Security Policies Overview	66
	Creating Security Policies	68
	Deploying Security Policies	74
	Managing Security Policies	79
	Viewing the Details of a Security Policy	80
	Modifying a Security Policy	81
	Deleting a Security Policy	81
	Searching for a Security Policy	81
	Viewing Job Details	81
	Decommissioning Security Policies	83
Chapter 10	NAT	85
	NAT Overview	85
	Creating a NAT Policy	87
	Create a Source NAT Rule	90
	Create a Static NAT Rule	93
	Provisioning a NAT Policy	95
	Decommissioning a NAT Policy	97
	Managing NAT Policies	98
	Modifying a NAT Policy	99
	Deleting a NAT Policy	99
	Managing NAT Pools	100
	Creating a NAT Pool	100
	Modifying a NAT Pool	101
	Deleting a NAT Pool	101
Chapter 11	IPsec VPNs	103
	VPN Proposals Overview	103
	Creating VPN Proposals	104
	Managing VPN Proposals	108
	Viewing the Details of a VPN Proposal	108
	Modifying a VPN Proposal	109
	Deleting a VPN Proposal	110
	Copying a VPN Proposal	111

Searching for a VPN Proposal	111
VPN Profiles Overview	112
Creating VPN Profiles	112
Managing VPN Profiles	118
Viewing the Details of a VPN Profile	119
Modifying a VPN Profile	120
Deleting a VPN Profile	121
Copying a VPN Profile	122
Searching for a VPN Profile	122
IPsec VPNs Overview	123
Creating IPsec VPNs	123
Site-To-Site	125
Hub-And-Spoke	126
Deploying IPsec VPNs	127
Managing IPsec VPNs	133
Modifying an IPsec VPN	134
Deleting an IPsec VPN	134
Decommissioning IPsec VPNs	135

Part 5

Index

Index	139
-----------------	-----

List of Figures

Part 1	Security Design Overview	
Chapter 3	Security Design Gadgets Overview	7
	Figure 1: Dashboard Gadget: Devices Used in Security Topology	8
	Figure 2: Dashboard Gadgets: Object Count	9
	Figure 3: Dashboard Gadget: Address Types	9
	Figure 4: Dashboard Gadget: Object Usage	10
	Figure 5: Dashboard Gadgets: Devices in Security Topology	10
	Figure 6: Dashboard Gadgets: Job Types	11
	Figure 7: Dashboard Gadgets: State of Jobs Run	11
	Figure 8: Dashboard Gadgets: Average Execution Time per Completed Job	12
Part 3	Object Builder	
Chapter 5	Applications and Application Groups	19
	Figure 9: Manage Applications Inventory Panel	20
	Figure 10: Create Application Window	21
	Figure 11: Create Application Groups Window	26
	Figure 12: Select Applications Window	27
Chapter 6	Security Domains	31
	Figure 13: Manage Security Domain Inventory Panel	32
	Figure 14: Create Security Domain Window	33
	Figure 15: Security Domain Detailed View	35
	Figure 16: Security Domain Hierarchy	37
Chapter 7	Addresses	39
	Figure 17: Manage Address Inventory Panel	40
	Figure 18: Create Address Window	41
	Figure 19: Audit Log Detail Popup Window	43
Part 4	Security Whiteboard	
Chapter 8	Security Topology	47
	Figure 20: Security Topology Designer Whiteboard	50
	Figure 21: Device Chooser Panel	52
	Figure 22: Add Objects Window	54
	Figure 23: Adding Ungrouped Devices into a Group	55
	Figure 24: Security Topology Designer Whiteboard: Logical Scape	58
Chapter 9	Security Policies	59
	Figure 25: Manage Policy Profiles Inventory Panel	61
	Figure 26: New Policy Profile Window	62

	Figure 27: New Policy Profile: Firewall Authentication Section	63
	Figure 28: New Policy Profile: Redirect Section	63
	Figure 29: Policy Profile Detail View Window	65
	Figure 30: Security Policy Designer Whiteboard	68
	Figure 31: Create Policy Window	69
	Figure 32: Add Rule Window	71
	Figure 33: Provision Security Policy Window	74
	Figure 34: Configuration Preview	74
	Figure 35: Viewing CLI Commands: Policy	75
	Figure 36: View XML Commands: Policy	76
	Figure 37: Manage Policies Inventory Panel	80
	Figure 38: Job Details Window	82
	Figure 39: Decommissioning a Security Policy	83
Chapter 10	NAT	85
	Figure 40: Manage NAT Policies Page	86
	Figure 41: Create NAT Policy Page	88
	Figure 42: List of Devices Between the Specified Endpoints	89
	Figure 43: NAT Rules	89
	Figure 44: Add NAT Rule Dialog Box	90
	Figure 45: Add Source NAT Rule	91
	Figure 46: Translation Parameters for IP/Subnet Option	92
	Figure 47: Translation Parameters for NAT Pool Option	92
	Figure 48: Advanced Settings	93
	Figure 49: Add Static NAT Rule	94
	Figure 50: Provision NAT Policy	95
	Figure 51: Decommission NAT Policy	98
	Figure 52: Create NAT Pool Page	100
	Figure 53: Delete NAT Pool Dialog Box	102
Chapter 11	IPsec VPNs	103
	Figure 54: Manage VPN Proposals Inventory Panel	104
	Figure 55: Create VPN Proposal Window	105
	Figure 56: Adding a Custom IKE Proposal	106
	Figure 57: Adding a Custom IPsec Proposal	107
	Figure 58: Viewing VPN Proposal Details	109
	Figure 59: Modifying a VPN Proposal	110
	Figure 60: Searching for a VPN Proposal	111
	Figure 61: Default VPN Profiles	113
	Figure 62: Creating a VPN Profile	113
	Figure 63: Choosing a Default VPN Proposal	114
	Figure 64: Choosing a Custom VPN Proposal	115
	Figure 65: Specifying IKE Settings	115
	Figure 66: Specifying Advanced IKE Settings	116
	Figure 67: Specifying Advanced IPsec Settings	117
	Figure 68: Specifying Connectivity Parameters	118
	Figure 69: Viewing the Details of a VPN Profile	120
	Figure 70: Modifying a VPN Profile	121
	Figure 71: Searching for a VPN Profile	122
	Figure 72: Create IPsec VPN:General Panel	124

Figure 73: Marking Endpoints for a VPN	126
Figure 74: VPN Overlay Over Topology	127
Figure 75: Provision VPN Window	128
Figure 76: View XML Commands:VPN	128
Figure 77: Viewing CLI Commands: VPN	129
Figure 78: IPSec VPN with an Intermediate Firewall	132
Figure 79: Policies Affected While Provisioning a VPN	133
Figure 80: Decommission VPN Window	135

List of Tables

	About the Documentation	xvii
	Table 1: Notice Icons	xvii
Part 1	Security Design Overview	
Chapter 2	Security Design Dashboard Overview	5
	Table 2: Security Design Workspaces	5
Part 4	Security Whiteboard	
Chapter 8	Security Topology	47
	Table 3: Security Topology Designer Toolbar Icons	50
	Table 4: Adding Addresses and Security Domains Using CSV Import	57
Chapter 9	Security Policies	59
	Table 5: Security Policy Designer Toolbar Icons	68
	Table 6: Security Policy Provision States	78
Chapter 10	NAT	85
	Table 7: Provision NAT Policy Table Descriptions	96
Chapter 11	IPsec VPNs	103
	Table 8: Default VPN Proposals	104
	Table 9: IPsec VPN Provision States	131

About the Documentation

- Junos Space Documentation and Release Notes on page xvii
- Documentation Conventions on page xvii
- Documentation Feedback on page xviii
- Requesting Technical Support on page xviii

Junos Space Documentation and Release Notes

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





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

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

Documentation Conventions

Table 1 on page xvii defines notice icons used in this documentation.

Table 1: Notice Icons

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

Documentation Feedback

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

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

Requesting Technical Support

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

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf> .
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/> .
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

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

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://www.juniper.net/alerts/>

- Join and participate in the Juniper Networks Community Forum:
<http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

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

Opening a Case with JTAC

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

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

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

PART 1

Security Design Overview

- Security Design Overview on page 3
- Security Design Dashboard Overview on page 5
- Security Design Gadgets Overview on page 7

CHAPTER 1

Security Design Overview

- Security Design Overview on page 3

Security Design Overview

Security Design is a Junos Space application that you can use to design your network security using a bottom-up approach. It significantly reduces your intervening time because you can create subconfiguration objects that you can use across multiple configurations. You can customize these for a specific configuration in which this object is used. A set of gadgets displayed on the dashboard graphically illustrate the critical factors related to your security design. These gadgets help you keep track of the objects created and their usage across security configurations easily and effectively.

The Security Design application is divided across two workspaces: Object Builder and Security Whiteboard.

- You can use the Object Builder workspace to prepare yourself for the security configuration
- You can use the Security Whiteboard workspace to configure your network security.

With the Object Builder workspace you can create subconfiguration Application, Network Address, and Security Domain objects and store them in the Junos Space database. You can access these objects from an inventory panel. You can clone objects easily without having to re-enter similar object parameters all over again. You can reuse these objects across multiple security configurations.

With the Security Whiteboard workspace you can create the actual security configurations. You can create a security topology to represent your physical network using a whiteboard-based design. You can drag and drop objects on the whiteboard and link them logically using a set of toolbar icons. You can also create IPsec VPNs and security policies using this workspace.

You can preview the Hub-And-Spoke or Site-To-Site VPN, as an overlay of the security topology, to ensure that you place the VPN strategically in your network. Security Design helps you create security policies in two ways. You can quickly create a security policy using a generic security policy profile object and a set of domain rules from the security domains that constitute a security policy. You can also create a detailed security policy which uses a customized security policy profile and customized rules which are applicable only to this security policy. You can also differentiate inherited rules versus additional

rules and generic security policy profile settings versus customized security policy profile settings using visual indicators.

For information about the using the Security Design application, see “Security Designer Dashboard Overview” on page 5.

CHAPTER 2

Security Design Dashboard Overview

- Security Design Dashboard Overview on page 5





Security Design Dashboard Overview

The Security Design dashboard graphically illustrates the devices used in the security topology. You can navigate to the Security Design dashboard in the following ways:

- Selecting Security Design from the Junos Space home page
- Selecting Security Design from the Application Switcher
- Selecting the Home icon from any page within the Security Design workspaces

The Security Design dashboard includes the Object Builder and Security Whiteboard workspaces. Table 2 on page 5 shows the workspace icons and the tasks that they perform.

Table 2: Security Design Workspaces

Icons	Workspace Name	Tasks
	Devices	Manage, discover, and add devices.
	Object Builder	Create, modify, delete, and copy security domains, addresses and applications.
	Security Whiteboard	Create security topology and security policies. Also used to create VPN proposals, VPN profiles and IPsec VPNs.
	Job Management	Manage and view job status.

The dashboard also includes gadgets that display information about objects and security configurations. To read more about gadgets in Security Design, see “Security Design Gadgets Overview” on page 7.

CHAPTER 3

Security Design Gadgets Overview

- Security Design Gadgets Overview on page 7

Security Design Gadgets Overview

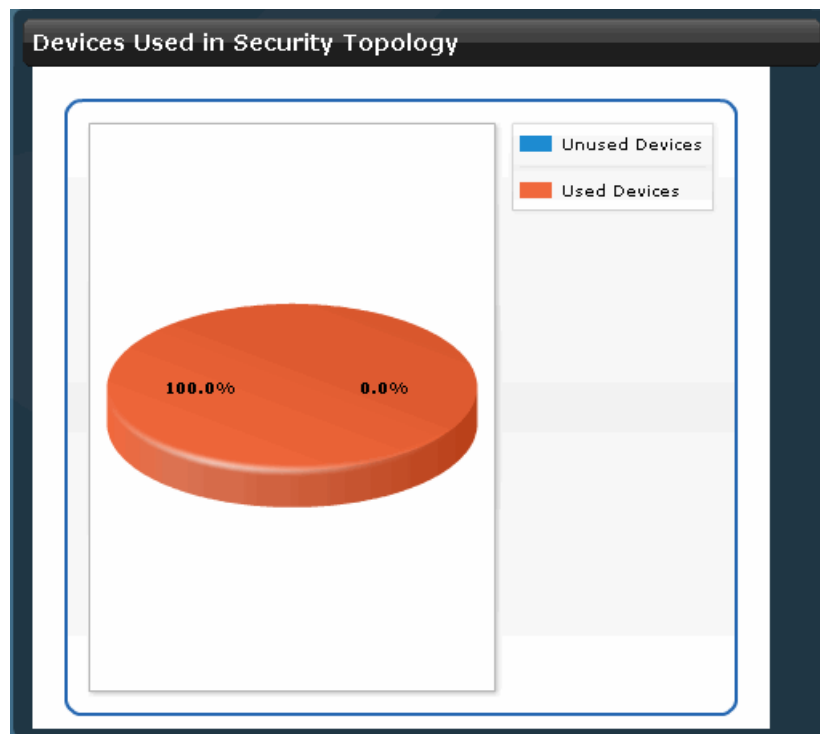
The Security Design dashboard displays gadgets with information that is updated automatically and immediately. You can move gadgets on the dashboard and resize them. These changes persist when you log out and log in to the Security Design application. The gadgets displayed on the Security Design dashboard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

1. Devices Used in Security Topology on page 7
2. Object Count on page 8
3. Address Types on page 9
4. Object Usage on page 9
5. Devices in Security Topology on page 10
6. Job Types on page 10
7. State of Jobs Run on page 11
8. Average Execution Time per Completed Job on page 11

Devices Used in Security Topology

You can view the Devices Used in the Security Topology gadget, as shown in Figure 1 on page 8, to learn the number of devices that are part of the security topology. You can use this gadget to keep a track of the number of devices used in your topology design.

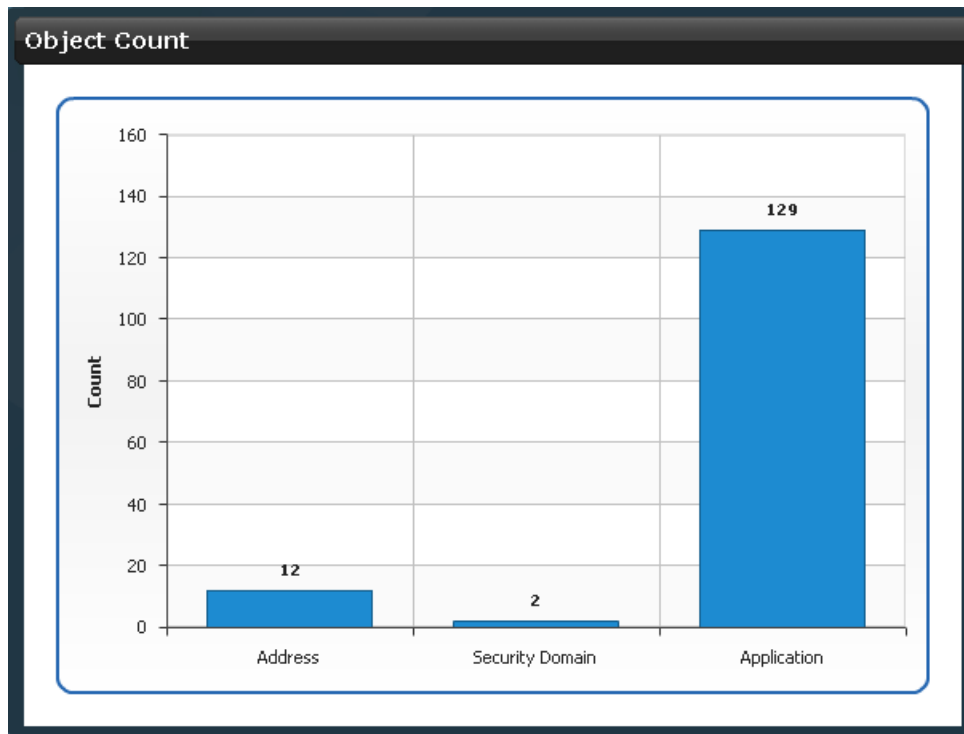
Figure 1: Dashboard Gadget: Devices Used in Security Topology



Object Count

You can view the Object Count gadget, as shown in Figure 2 on page 9, to learn the number of objects that are created from the Object Builder workspace. You can use this gadget to keep a track of the objects available to create a security topology, IPsec VPNs, or security policies.

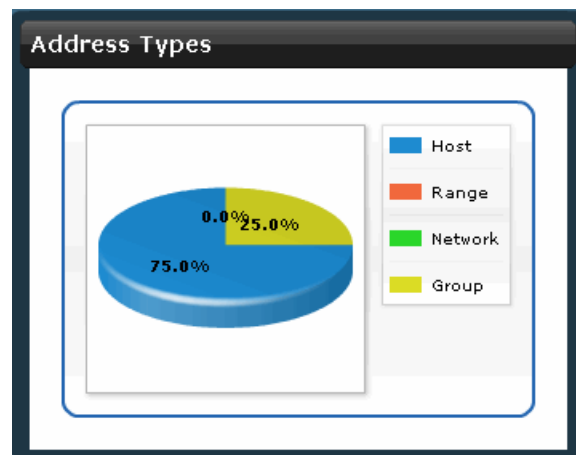
Figure 2: Dashboard Gadgets: Object Count



Address Types

You can view the Address Types gadget, as shown in Figure 3 on page 9, to learn the distribution among the different address types created using the Address Creation Wizard.

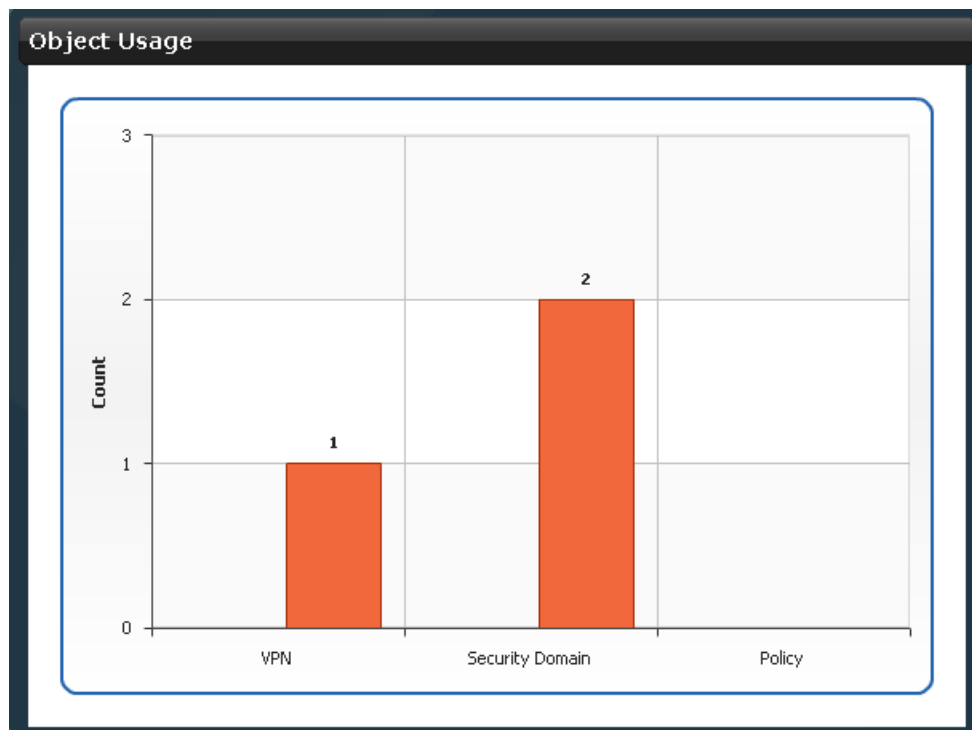
Figure 3: Dashboard Gadget: Address Types



Object Usage

You can view the Object Usage gadget, as shown in Figure 4 on page 10, to learn the number of objects used to create VPNs, security domains, or security policies.

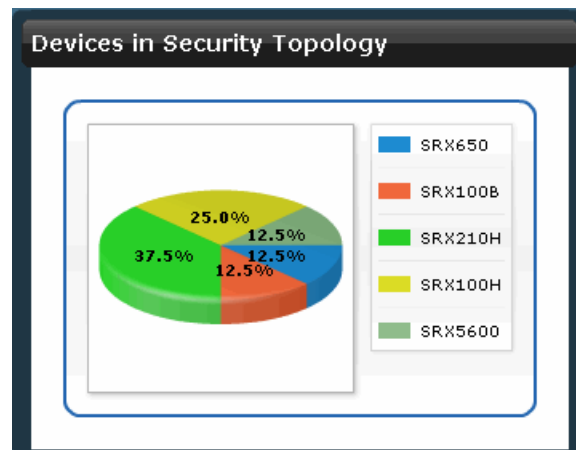
Figure 4: Dashboard Gadget: Object Usage



Devices in Security Topology

You can view the Devices in Security Topology gadget, as shown in Figure 5 on page 10, to learn the different types of devices used to create the security topology.

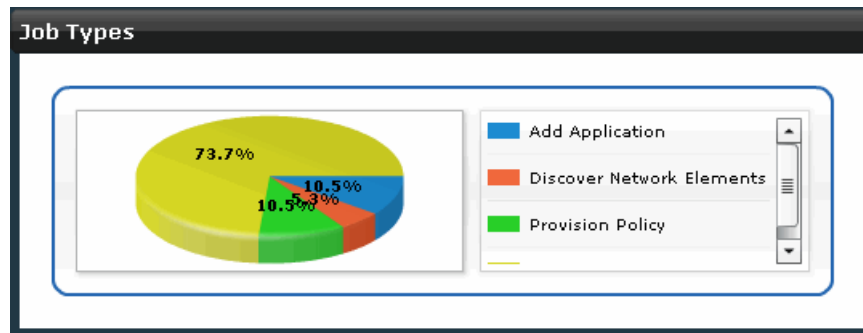
Figure 5: Dashboard Gadgets: Devices in Security Topology



Job Types

You can view the Job Types gadget, as shown in Figure 6 on page 11, to learn the type of jobs performed using Security Design.

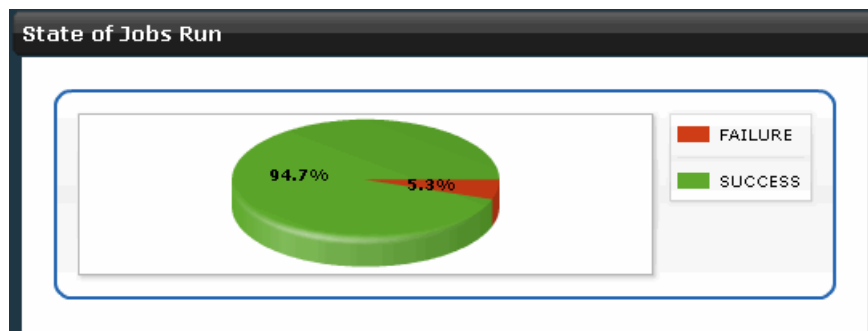
Figure 6: Dashboard Gadgets: Job Types



State of Jobs Run

You can view the State of Jobs Run gadget, as shown in Figure 7 on page 11, to learn the status of the jobs that your Security Design tasks have initiated.

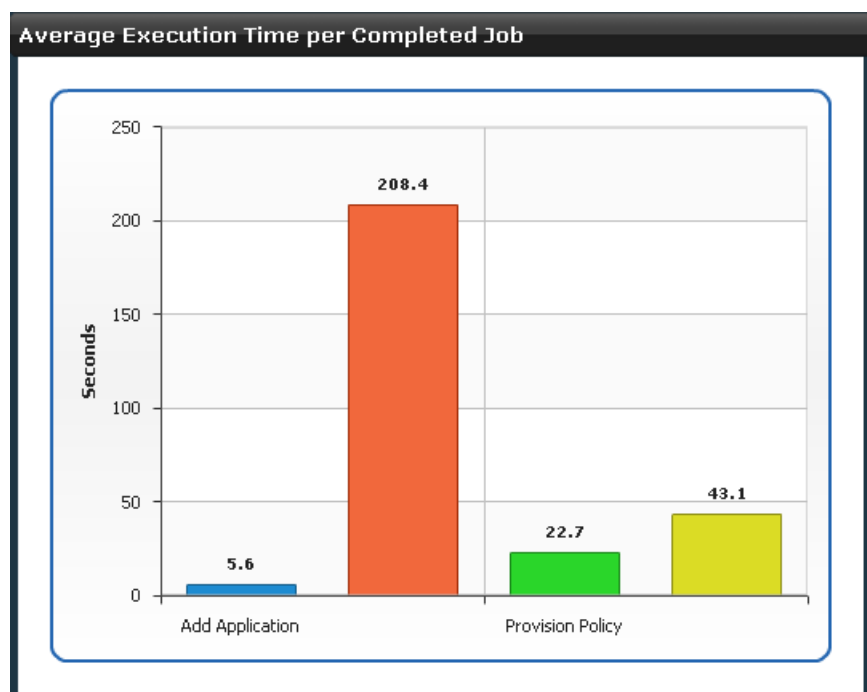
Figure 7: Dashboard Gadgets: State of Jobs Run



Average Execution Time per Completed Job

You can view the Average Execution Time per Completed Job gadget, as shown in Figure 8 on page 12, to learn the average time that your Security Design tasks have taken to run specific job types.

Figure 8: Dashboard Gadgets: Average Execution Time per Completed Job



PART 2

Getting Started

- [Getting Started with Security Design on page 15](#)

CHAPTER 4

Getting Started with Security Design

- Getting Started with Security Design on page 15

Getting Started with Security Design

The **Getting Started** assistant is a section on the sidebar that provides instructions on how to perform tasks related to IPsec VPN configuration and security policy configuration in Security Design.

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

1. Provisioning an IPsec VPN on page 15
2. Provisioning Firewall Policies on page 16

Provisioning an IPsec VPN

In general, to provision an IPsec VPN::

1. Discover devices.
For information about how to discover devices, see the Discovering Devices section in the Junos Space Network Application Platform User Guide.
2. Create addresses.
For information about how to create addresses, see “Creating Addresses” on page 40.
3. Create security domains.
For information about how to create security domains, see “Creating Security Domains” on page 32.
4. Create a security topology.
For information about how to create a security topology, see “Creating a Security Topology” on page 49.
5. Create a VPN profile.
For information about how to create a VPN profile, see “Creating VPN Profiles” on page 112.
6. Create a VPN proposal.
For information about how to create a VPN proposal, see “Creating VPN Proposals” on page 104.
7. Create an IPsec VPN.

For information about how to create an IPsec VPN, see “Creating IPsec VPNs” on page 123.

8. Provision the IPsec VPN.

For information about how to provision the IPsec VPN, see “Deploying IPsec VPNs” on page 127.

Provisioning Firewall Policies

The steps to provision firewall policies are:

1. Discover devices.

For information about how to discover devices, see the Discovering Devices section in the Junos Space Network Application Platform User Guide.

2. Create addresses.

For information about how to create addresses, see “Creating Addresses” on page 40.

3. Create security domains.

For information about how to create security domains, see “Creating Security Domains” on page 32.

4. Create a security topology.

For information about how to create a security topology, see “Creating a Security Topology” on page 49.

5. Create a policy profile.

For information about how to create a policy profile, see “Creating Security Policy Profiles” on page 61.

6. Create a applications.

For information about how to create an application, see “Creating Applications” on page 20.

7. Create firewall policies.

For information about how to create firewall policies, see “Creating Security Policies” on page 68.

8. Provision firewall policies.

For information about how to provision firewall policies, see “Deploying Security Policies” on page 74.

PART 3

Object Builder

- [Object Builder Overview on page 17](#)
- [Applications and Application Groups on page 19](#)
- [Security Domains on page 31](#)
- [Addresses on page 39](#)

Object Builder Overview

You can use the Object Builder workspace in Security Design to create security policy-related objects like security domains, addresses, and applications. These objects are stored in the Junos Space database. You can reuse them with multiple security policies. This makes the security policy design more structured and avoids the need to create the security policy-related objects during the whiteboard-based security policy design.

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

- Addresses
- Applications and application groups
- Security domains

Related Documentation

- [Addresses Overview on page 39](#)
- [Application and Application Groups Overview on page 19](#)
- [Security Domains Overview on page 31](#)

CHAPTER 5

Applications and Application Groups

- Application and Application Groups Overview on page 19
- Creating Applications on page 20
- Managing Applications on page 23
- Creating Application Groups on page 25
- Managing Application Groups on page 27

Application and Application Groups Overview

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

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

You can group application objects to form an application group using the Application Group Creation Wizard. Junos Space creates an object in the Junos Space database to represent an application or an application group. Security domains use these objects to allow or block applications in the domain.

Junos Space provides Juniper Networks defined application objects for commonly used applications.



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

Related Documentation

- Creating Applications on page 20
- Creating Application Groups on page 25
- Managing Applications on page 23

- Managing Application Groups on page 27

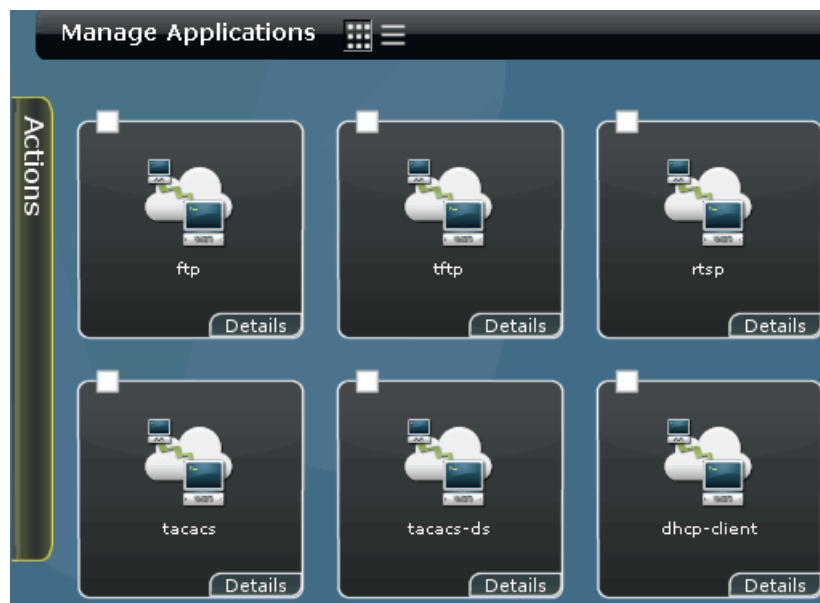
Creating Applications

To create a new application:

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

The **Manage Applications** inventory panel is displayed with the icons for all the applications, as shown in Figure 9 on page 20.

Figure 9: Manage Applications Inventory Panel



2. From the task ribbon, select the **Create Application** icon.

The **Create Application** window is displayed, as shown in Figure 10 on page 21.

Figure 10: Create Application Window

Create Application

Name:

Category:

Description:

Protocols: + ✎ ✖

Name	Detail
------	--------

3. In the **Name** field, enter a name for the new application.
4. In the **Category** field, enter a category for the new application.
5. In the **Description** field, enter a description for the new application.
6. In the **Protocols** section, click the **Add** icon to add a new protocol.

The **New Protocol** dialog box is displayed with default values.

7. In the **Name** section, enter a name for the new protocol.
8. In the **Inactivity Timeout** section, enter a value in seconds.

The default value is 60 seconds.

9. From the **Type** drop-down menu, select a protocol type.

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

- TCP - Transmission Control Protocol
 - a. From the **Type** drop-down menu, select **TCP** as the protocol type.

The **New Protocol** dialog box displays the fields relevant to the protocol type.

- b. From the **ALG** drop-down menu, select the protocol you want to use.

- c. In the **Source Port** field, enter a range of TCP source ports the application uses.
- d. In the **Destination Port** field, enter a range of TCP destination ports the application uses.
- UDP - User Datagram Protocol
 - a. From the **Type** drop-down menu, select UDP as the protocol type.

The **New Protocol** dialog box displays the fields relevant to the protocol type.
 - b. From the **ALG** drop-down menu, select the protocol you want to use.
 - c. b. In the **Source Port** field, enter a range of UDP source ports the application uses.
 - d. In the **Destination Port** field, enter a range of UDP destination ports the application uses.
- ICMP - Internet Control Message Protocol
 - a. From the **Type** drop-down menu, select **ICMP** as the protocol type.

The **New Protocol** dialog box displays the fields relevant to the protocol type.
 - b. In the **ICMP Type** field, enter a value pertaining to the ICMP message you want to display.
 - c. In the **ICMP Code** field, enter a value associated with the ICMP type you have specified.
- SUN - RPC - Remote Procedure Call
 - a. From the **Type** drop-down menu, select **SUN—RPC** as the protocol type.

The **New Protocol** dialog box displays the fields relevant to the protocol type.
 - b. In the **RPC Program Number** field, enter a value corresponding to the RPC service you want to use.
 - c. Select the **TCP** or **UDP** radio button to specify an appropriate protocol type in the **Protocol Type** field.
- MS - RPC - Remote Procedure Call
 - a. From the **Type** drop-down menu, select **MS—RPC** as the protocol type.

The **New Protocol** dialog box displays the fields relevant to the protocol type.
 - b. In the **uuid** field, enter the universally unique ID corresponding to the RPC service you want to use.
 - c. Select the **TCP** or **UDP** radio button to specify an appropriate protocol type in the **Protocol Type** field.
- Other Protocols

- a. From the **Type** drop-down menu, select **Other** as the protocol type.
The **New Protocol** dialog box displays the fields relevant to the protocol type.
- b. From the **ALG** drop-down menu, select the protocol you want to use.
- c. In the **Source Port** field, enter a range of TCP source ports the application uses.
- d. In the **Destination Port** field, enter a range of TCP destination ports the application uses.
- e. In the **Protocol Number** field, enter the protocol number of the protocol you want to use.

This number is specified in the Protocol field for IPv4 packets and the Next Header field for IPv6 packets.

10. Click **Add** in the **New Protocol** dialog box.

11. Click **Create** to create a new application.

The new application you have created is displayed in the **Manage Applications** inventory panel.

Related Documentation

- Application and Application Groups Overview on page 19
- Managing Applications on page 23
- Creating Application Groups on page 25
- Managing Application Groups on page 27

Managing Applications

You can view, delete, or modify applications listed in the **Manage Application** inventory panel.

To open the **Manage Application** inventory panel:

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

The **Manage Applications** inventory panel is displayed. All applications created are listed by default, in the graphical view.

You can either right-click or use the Actions Drawer to manage an application. For more information about using the Actions Drawer, see [Inventory Pages Overview](#)

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

1. Viewing the Details of an Application on page 24
2. Modifying an Application on page 24
3. Deleting an Application on page 24
4. Searching for an Application on page 25

Viewing the Details of an Application

To view the details of an application:

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

The **Manage Applications** inventory panel is displayed.

2. Double-click the icon for the application whose details you intend to view.

The details of the application are displayed in the **Application Detailed View** window.

The **Application Detailed View** window lists the name, category, description and protocols used in this application.

3. Click **Close**.

Modifying an Application

To modify an application you have created:

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

The **Manage Applications** inventory panel is displayed.

2. Right-click the application you want to modify and click the **Modify Application** link from the contextual menu.

This action redirects you to the window that you used to create a new application.

You can modify all the fields on this window, except the **Name** field.

3. In the **Category** field, enter a new category.
4. In the **Description** field, enter a new description.
5. Make necessary changes in the **Protocols** section.

You can also edit or modify the existing protocols in the **Protocols** section.

- To edit a protocol, select the protocol you want to edit and click the **Edit** icon. Make the necessary changes and click **OK**.
- To delete a protocol, select the protocol you want to delete and click the **Delete** icon.

6. Click **Modify** to save the changes made to this application.

Deleting an Application

To delete an application you have created:

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

The **Manage Applications** inventory panel is displayed.

2. Right-click the application you want to delete and click the **Delete Applications** link from the contextual menu.

The **Delete** dialog box is displayed

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

Searching for an Application

To search for an application you have created:

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

The **Manage Applications** inventory panel is displayed.

2. In the **Search** field, enter the name of application you want to search.

3. Click the magnifying glass icon next to **Search** field.

The **Manage Application** inventory panel is populated with the applications matching your search criterion.

Related Documentation

- Application and Application Groups Overview on page 19
- Creating Applications on page 20

Creating Application Groups

To create a new application group:

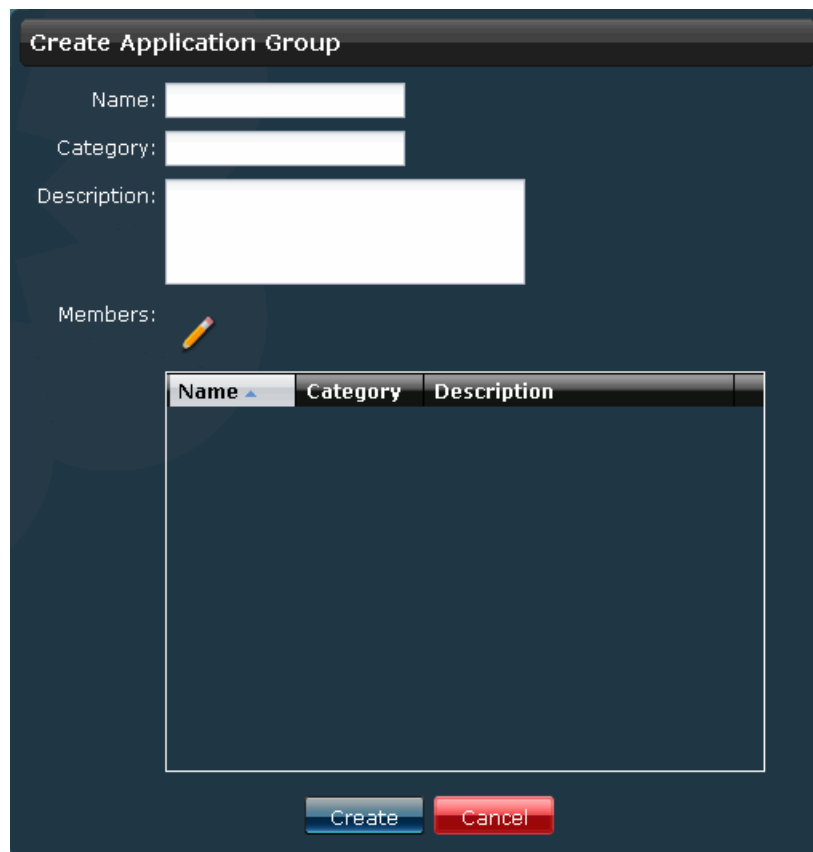
1. From the **Security Design** task ribbon, select **Object Builder > Applications**.

The **Manage Applications** inventory panel is displayed with the icons for all the applications and application groups.

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

The **Create Application Group** window is displayed, as shown in Figure 11 on page 26.

Figure 11: Create Application Groups Window



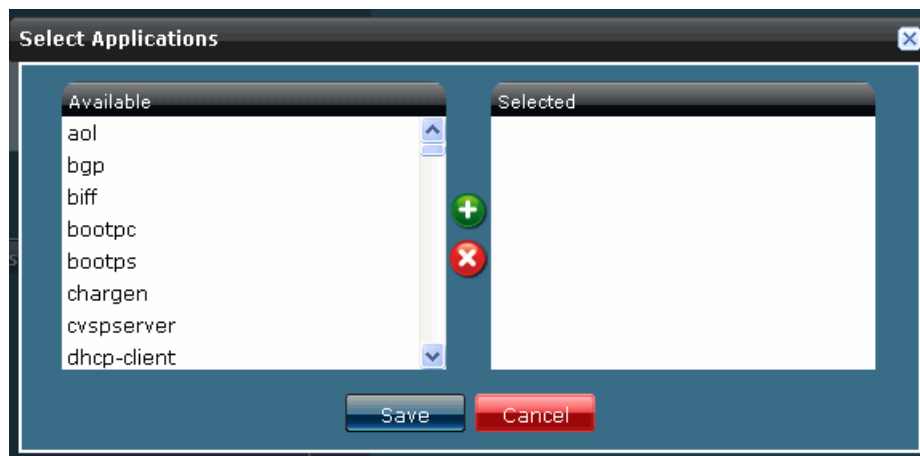
The 'Create Application Group' dialog box features a dark blue background. At the top, the title 'Create Application Group' is displayed in a dark bar. Below the title, there are three input fields: 'Name:' with a single-line text box, 'Category:' with a single-line text box, and 'Description:' with a larger multi-line text box. Under the 'Members:' label, there is a small yellow pencil icon. Below this is a table with three columns: 'Name', 'Category', and 'Description'. The table is currently empty. At the bottom of the dialog, there are two buttons: a blue 'Create' button and a red 'Cancel' button.

Name	Category	Description
------	----------	-------------

3. In the **Name** field, enter a name for the new application group.
4. In the **Description** field, enter a description for the new application group.
5. In the **Members** section, click the Add icon to add a new application to this application group.

The **Select Applications** dialog box is displayed, as shown in Figure 12 on page 27.

Figure 12: Select Applications Window



6. From the **Available** section of the dialog box, select the application you want to group, and click the Add icon.

The application you have selected is displayed in the **Selected** section of the dialog box. Repeat Steps 5 and 6 to add more applications in this application group.

7. Click **Create**.

The application group you have created is displayed in the **Manage Applications** inventory panel.

Related Documentation

- Application and Application Groups Overview on page 19
- Managing Application Groups on page 27
- Creating Applications on page 20
- Managing Applications on page 23

Managing Application Groups

You can view, delete, or modify application groups listed in the **Manage Applications** inventory panel.

To open the **Manage Applications** inventory panel:

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

The **Manage Applications** inventory panel is displayed. All application groups created are listed by default, in the graphical view.

You can either right-click or use the Actions Drawer to manage an application group. For more information about using the Actions Drawer, see [Inventory Pages Overview](#)

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

1. Viewing the Details of an Application Group on page 28
2. Modifying an Application Group on page 28
3. Deleting an Application Group on page 29
4. Searching for an Application Group on page 29

Viewing the Details of an Application Group

To view the details of an application group:

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

The **Manage Applications** inventory panel is displayed.

2. Double-click the icon for the application group whose details you intend to view.

The details of the application group are displayed in the **Application Detailed View** window. The **View** window lists the name, description, category and the protocols used in this application group.

3. Click **OK**.

Modifying an Application Group

To modify an application group you have created:

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

The **Manage Applications** inventory panel is displayed.

2. Right-click the application group you want to modify and click the **Modify Application** link from the contextual menu.

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

3. In the **Description** field, enter a new description.
4. In the **Category** field, enter a new category.
5. In the **Members** section, make appropriate changes to the applications used in this group.
6. Click **Modify** to save the changes made to this application group.

Deleting an Application Group

To delete an application group you have created:

1. From the **Security Design** task ribbon, select **Object Builder > Applications**.
The **Manage Applications** inventory panel is displayed.
2. Right-click the application group you want to delete and click the **Delete Applications** link from the contextual menu.
The **Delete** dialog box is displayed.
3. Select the application group you want to delete and click **Delete**.

Searching for an Application Group

To search for an application group you have created:

1. From the **Security Design** task ribbon, select **Object Builder > Applications**.
The **Manage Applications** inventory panel is displayed.
2. In the **Search** field, enter the name of application group you want to search.
3. Click the magnifying glass icon next to **Search** field.
The **Manage Applications** inventory panel is populated with the application groups matching your search criterion.

Related Documentation

- Application and Application Groups Overview on page 19
- Creating Application Groups on page 25

CHAPTER 6

Security Domains

- [Security Domains Overview on page 31](#)
- [Creating Security Domains on page 32](#)
- [Managing Security Domains on page 34](#)
- [Viewing Security Domain Hierarchy on page 36](#)

Security Domains Overview

You can use the Security Domain Creation Wizard to create a security domain that contains applications hosted by the domain and applications that are blocked to and from the domain. You can also choose to allow intra-domain traffic in a domain that is spread across different locations.

Junos Space creates an object in the Junos Space database to represent the security domain. You can use these security domain objects as endpoints to create a security policy. After the security policy is created, you can configure the direction in which the application data flows between two domains for that policy.

Related Documentation

- [Creating Security Domains on page 32](#)
- [Managing Security Domains on page 34](#)
- [Viewing Security Domain Hierarchy on page 36](#)

Creating Security Domains

To create a new security domain:

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

The **Manage Security Domain** inventory panel is displayed with the icons for all security domains, as shown in Figure 13 on page 32.

Figure 13: Manage Security Domain Inventory Panel



2. From the task ribbon, select the **Add New Security Domain** icon.

The **Create Security Domain** window is displayed, as shown in Figure 14 on page 33.

Figure 14: Create Security Domain Window

Create Security Domain

Name:

Description:

☐

Allow Intra-Domain Traffic

Blacklisted Applications:

Name	Category	Description
------	----------	-------------

Domain Association

Parent Domain:

Please select ...

Create

Cancel

3. In the **Name** field, enter a name for the new security domain.
4. In the **Description** field, enter a description for the new security domain.
5. If you want to allow intra-domain traffic in a domain that is spread across different locations, select the **Allow Intra-Domain Traffic** check box.



NOTE: You can use the **Allow Intra-Domain Traffic** option to enable seamless communication across all subnets located across your network.

6. In the **Blacklisted Applications** section of the **Create Security Domain** window, click the **Add** icon to add the applications you want to blacklist in this domain.

The **Select Applications** window is displayed.

7. From the **Available** section of the dialog box, select the application you want to host, and click the right arrow.

The application you have selected is displayed in the **Selected** section of this dialog box.



NOTE: This action restricts access to these applications in both directions for the domain they are hosted in. This cannot be overridden by security policies.

8. From the **Parent Domain** drop-down menu in the **Domain Association** section, select the parent domain for this security domain.

The security domain you are now creating will be a subdomain to the parent domain you select from the drop-down menu.

9. Click **Create**.

The security domain you have created is displayed in the **Manage Security Domain** inventory panel.



NOTE: If you migrating to version 2.0 from previous versions, the hosted applications will be migrated as user rules.

Related Documentation

- Security Domains Overview on page 31
- Managing Security Domains on page 34
- Viewing Security Domain Hierarchy on page 36

Managing Security Domains

You can view, delete, or modify security domains listed in the **Manage Security Domain** inventory panel.

To open the **Manage Security Domain** inventory panel:

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

The **Manage Security Domain** inventory panel is displayed. All security domains created are listed by default, in the graphical view.

You can either right-click or use the Actions Drawer to manage a security domain. For more information about using the Actions Drawer, see [Inventory Pages Overview](#)

You can perform the following tasks in the **Manage Security Domain** space:

1. Viewing the Details of a Security Domain on page 35
2. Modifying a Security Domain on page 35
3. Deleting a Security Domain on page 36
4. Searching for a Security Domain on page 36

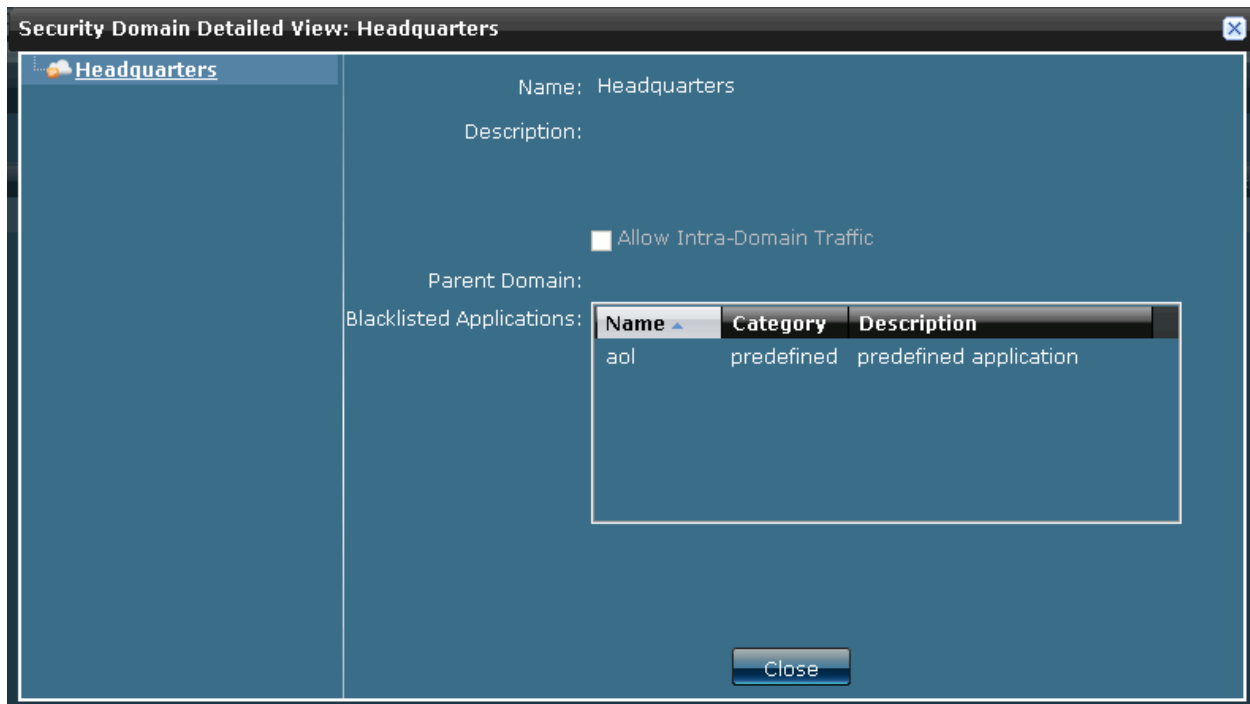
Viewing the Details of a Security Domain

To view the details of a security domain:

1. From the **Security Design** task ribbon, select **Object Builder > Security Domain**.
The **Manage Security Domain** inventory panel is displayed.
2. Double-click the icon for the security domain whose details you intend to view.

The details of the security domain are displayed in the **Security Domain Detailed View** window, as shown in Figure 15 on page 35. The **Security Domain Detailed View** window lists the name, description, hosted applications and the blacklisted applications in this security domain.

Figure 15: Security Domain Detailed View



3. Click **Close**.

Modifying a Security Domain

To modify a security domain you have created:

1. From the **Security Design** task ribbon, select **Object Builder > Security Domain**.
The **Manage Security Domain** inventory panel is displayed.
2. Right-click the security domain you want to modify and click the **Modify Security Domain** link from the contextual menu.

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

3. In the **Description** field, enter a new description.
4. Make appropriate changes in the **Hosted Applications** section of the **Create Security Domain** window.
5. Make appropriate changes in the **Blacklisted Applications** section of the **Create Security Domain** window.
6. Click **Modify** to save the changes made to this security domain.

Deleting a Security Domain

To delete a security domain you have created:

1. From the **Security Design** task ribbon, select **Object Builder > Security Domain**.
The **Manage Security Domain** inventory panel is displayed.
2. Right-click the security domain you want to delete and click the **Delete Security Domain** link from the contextual menu.
The **Delete** dialog box is displayed.
3. Select the security domain you want to delete and click **Delete**.

Searching for a Security Domain

To search for a security domain you have created:

1. From the **Security Design** task ribbon, select **Object Builder > Security Domain**.
The **Manage Security Domain** inventory panel is displayed.
2. In the **Search** field, enter the name of security domain you want to search.
3. Click the magnifying glass icon next to the **Search** field.
The **Manage Security Domain** inventory panel is populated with the security domains matching your search criterion.

Related Documentation

- Security Domains Overview on page 31
- Creating Security Domains on page 32
- Viewing Security Domain Hierarchy on page 36

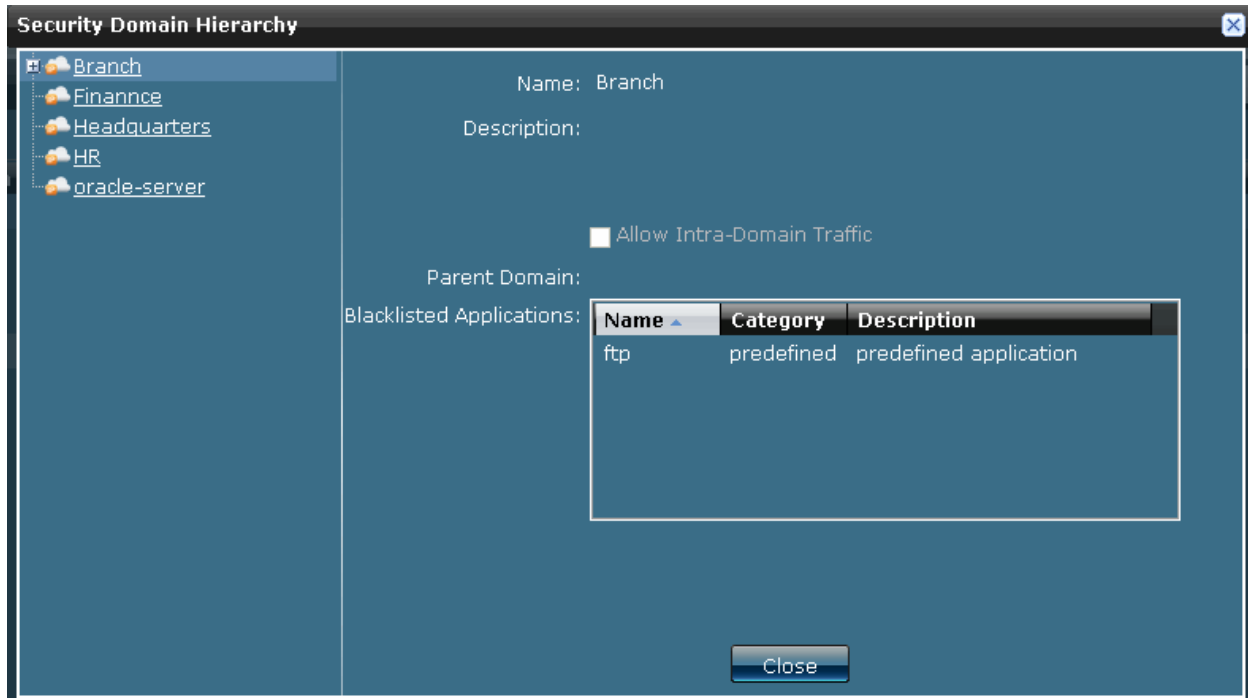
Viewing Security Domain Hierarchy

To view the security domain hierarchy:

1. From the **Security Design** task ribbon, select **Object Builder > Security Domains**.
The **Manage Security Domain** inventory panel is displayed with the icons for all security domains.
2. Click the security domain whose domain hierarchy you want to view and click the **View Domain Hierarchy** link from the Actions drawer.

The **Security Domain Hierarchy** window is displayed, as shown in Figure 16 on page 37. This window lists the hierarchy of the security domains.

Figure 16: Security Domain Hierarchy



- Related Documentation**
- Security Domains Overview on page 31
 - Creating Security Domains on page 32
 - Managing Security Domains on page 34

CHAPTER 7

Addresses

- [Addresses Overview on page 39](#)
- [Creating Addresses on page 40](#)
- [Managing Addresses on page 42](#)

Addresses Overview

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

You can group address objects to form an address group using the Address Group Creation Wizard. Junos Space creates an object in the Junos Space database to represent an address or an address group. You can use these addresses and address groups to create a security topology.

Related Documentation

- [Creating Addresses on page 40](#)
- [Managing Addresses on page 42](#)

Creating Addresses

To create a new address:

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

The **Manage Address** inventory panel is displayed with the icons for all addresses and the address groups, as shown in Figure 17 on page 40.

Figure 17: Manage Address Inventory Panel



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

The **Create Address** window is displayed, as shown in Figure 18 on page 41.

Figure 18: Create Address Window

The screenshot shows the 'Create Address' window with the following elements:

- Title Bar:** Create Address
- Name:** A text input field.
- Description:** A larger text input field.
- Type:** Three radio buttons: Host (selected), Range, and Network.
- IP:** A text input field.
- Host name:** A text input field.
- Resolution Arrows:** Two green circular arrows between the IP and Host name fields. The left arrow is labeled 'Get IP' and the right arrow is labeled 'Get Hostname'.
- Security Domain Association:** A section with a blue expand/collapse icon and a 'Domains' drop-down menu showing 'Please select ...'.
- Buttons:** 'Create' (blue) and 'Cancel' (red) buttons at the bottom.

3. In the **Name** field, enter a name for the new address.
4. In the **Description** field, enter a description for the new address.
5. You can direct Junos Space to resolve an IP address to a hostname or resolve a hostname to an IP address.
 - To specify an IP address as the address type, select the **Host** radio button and enter the IP address in the **IP** field.
 - To specify a hostname as the address type, select the **Host** radio button and enter the hostname in the **Host Name** field.
 - To specify an IP address range, select the **Range** radio button and enter the IP ranges in the **Start IP** and **End IP** fields.
 - To specify a network as an address type, select the **Network** radio button and enter the network address in the **IP** and **Netmask** fields.



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

6. From the **Domains** drop-down menu in the **Security Domain Association** section, select the security domains you want to associate this address with.

You can view the security domains with which this address is associated in the **Domains** drop-down menu.
7. Click **Create** to create a new address.

The new address you have created is displayed in the **Manage Address** inventory panel.

- Related Documentation**
- [Addresses Overview on page 39](#)
 - [Managing Addresses on page 42](#)

Managing Addresses

You can view, delete, or modify addresses listed in the **Manage Address** inventory panel.

To open the **Manage Address** inventory panel:

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

The **Manage Address** inventory panel is displayed. All addresses created are listed by default, in the graphical view.

You can either right-click or use the Actions Drawer to manage an address. For more information about using the Actions Drawer, see [Inventory Pages Overview](#)

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

1. [Viewing the Details of an Address on page 42](#)
2. [Modifying an Address on page 42](#)
3. [Deleting an Address on page 44](#)
4. [Searching for an Address on page 44](#)

Viewing the Details of an Address

To view the details of an address:

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

The **Manage Address** inventory panel is displayed.

2. Double-click the icon for the address whose details you intend to view.

The details of the address are displayed in the **Address Detailed View** window. The **Address Detailed View** window lists the name, description, and the IP address/host name specified for this address.

3. Click **Close**.

Modifying an Address

To modify an address you have created:

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

The **Manage Address** inventory panel is displayed.

2. Right-click the address you want to modify and click the **Modify Address** link from the contextual menu.

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

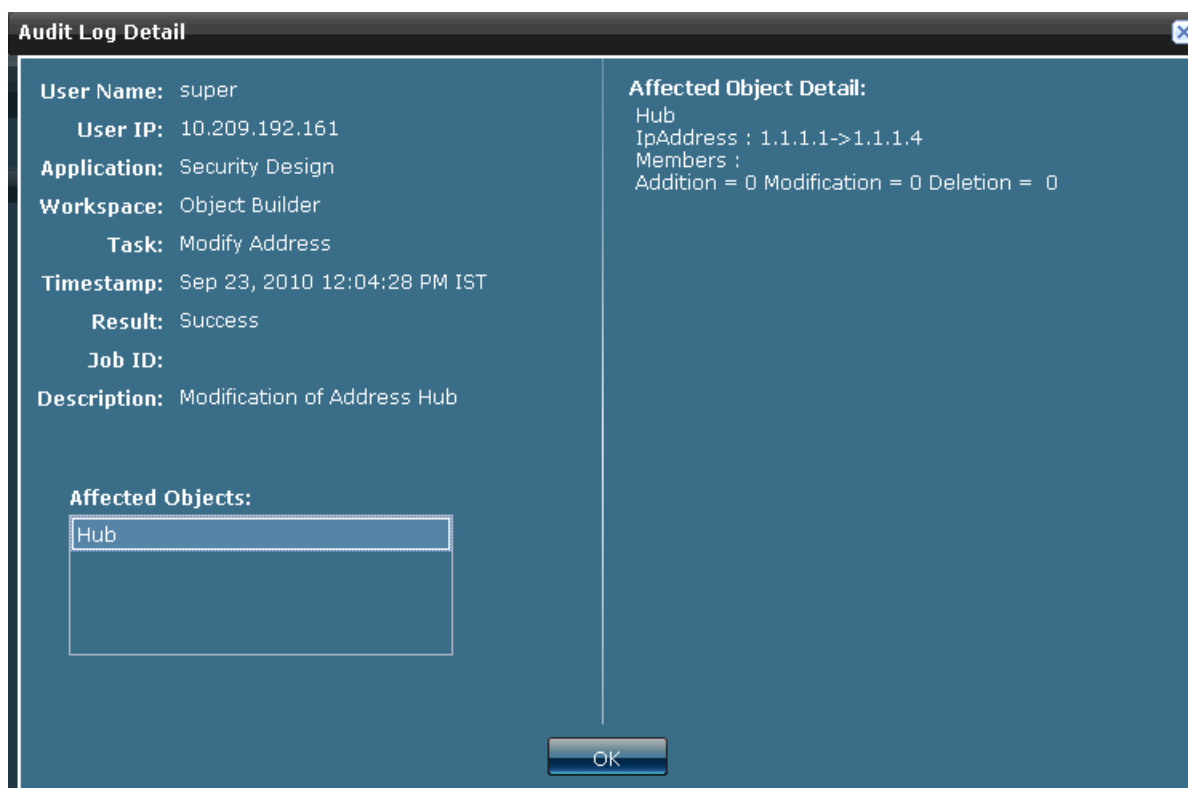
3. In the **Description** field, enter a new description.
4. Enter a new value for the **Address Type** you specified earlier in the appropriate field (**IP Address** field if you have chosen IP Address as the **Address Type** or hostname if you have chosen **Host Name** as the **Address Type**).
5.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



NOTE: You can view the details of the modified object in the Audit Logs workspace in the Network Application Platform application. You can see the difference in the object before and after the modification. For more information about viewing the Audit Logs, see [Viewing Audit Logs](#).

To view the audit log pertaining to the Modify Address task, double-click the audit log entry. The Audit Log Detail popup is displayed, as shown in Figure 19 on page 43.

Figure 19: Audit Log Detail Popup Window



Deleting an Address

To delete an address you have created:

1. From the **Security Design** task ribbon, select **Object Builder > Address**.
The **Manage Address** inventory panel is displayed.
2. Right-click the address you want to delete and click the **Delete Addresses** link from the contextual menu.
The **Delete** dialog box is displayed.
3. Select the address you want to delete and click **Delete**.

Searching for an Address

To search for a address you have created:

1. From the **Security Design** task ribbon, select **Object Builder > Address**.
The **Manage Address** inventory panel is displayed.
2. In the **Search** field, enter the name of address you want to search.
3. Click the magnifying glass icon next to **Search** field.
The **Manage Address** inventory panel is populated with the addresses matching your search criterion.

- Related Documentation**
- [Addresses Overview on page 39](#)
 - [Creating Addresses on page 40](#)

PART 4

Security Whiteboard

- Security Whiteboard Overview on page 45
- Security Topology on page 47
- Security Policies on page 59
- NAT on page 85
- IPsec VPNs on page 103

Security Whiteboard Overview

You can use the Security Whiteboard workspace in Security Design to create a security topology, IPsec VPNs, and security policies.

With the Security Topology Designer you can create a graphical view of the security aspect of the network, which you can use 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 in 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 among multiple security domains. You can associate the applications hosted by a security domain and the addresses associated with the security domain in real time.

Related Documentation

- Security Topology Overview on page 47
- Security Policy Profiles Overview on page 59
- Security Policies Overview on page 66
- NAT Overview on page 85
- VPN Proposals Overview on page 103
- VPN Profiles Overview on page 112
- IPSec VPNs Overview on page 123

CHAPTER 8

Security Topology

- Security Topology Overview on page 47
- Creating a Security Topology on page 49
- Changing Topology Scapes on page 57

Security Topology Overview

Security topology is a logical map that depicts the interconnectivity 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 to configure firewall policies on your security devices.

You can use the Security Topology Designer 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. You can also use the Security Topology Designer 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. You can choose security devices, security domains, and addresses from their individual object chooser panels. You can configure the interfaces used for communication after the components are linked in the topology design.

Security Topology Designer provides the following features 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 Documentation**
- [Creating a Security Topology on page 49](#)
 - [Changing Topology Scapes on page 57](#)

Creating a Security Topology

To navigate to the Security Topology Designer Whiteboard:

1. From the **Security Design** task ribbon, select **Security Whiteboard > Security Topology**.

The **Security Topology Designer Whiteboard** is displayed, as shown in Figure 20 on page 50.






By default, the Security Topology Designer Whiteboard is displayed in the Physical scape. You can add addresses and devices in this scape and associate them with one another. To view the Logical scape, which displays the respective domain associations, you should change the scape. For more information about changing scapes, see “Changing Topology Scapes” on page 57.

Figure 20: Security Topology Designer Whiteboard



The toolbar on the left displays a set of functionalities used to design the security topology, as listed in Table 3 on page 50.

Table 3: Security Topology Designer Toolbar Icons

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

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

You can use the Select:Page and Select:All links to select multiple objects simultaneously. You can use the Clear:Page and Clear:All links 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, and device groups used to create the topology.

You can drag and drop and interconnect the devices and addresses in the following ways:

1. Dragging and Dropping Security Devices on page 51
2. Connecting Security Devices on page 52
3. Dragging and Dropping Addresses on page 53
4. Associating Addresses with Security Devices on page 53
5. Creating Device Groups on page 54
6. Moving Ungrouped Devices into a Device Group on page 54
7. Removing Devices from a Device Group on page 55
8. Searching for Devices and Addresses in the Topology on page 55
9. Creating Group Links on Device Groups on page 56
10. Adding Addresses and Security Domains Using CSV Import on page 56

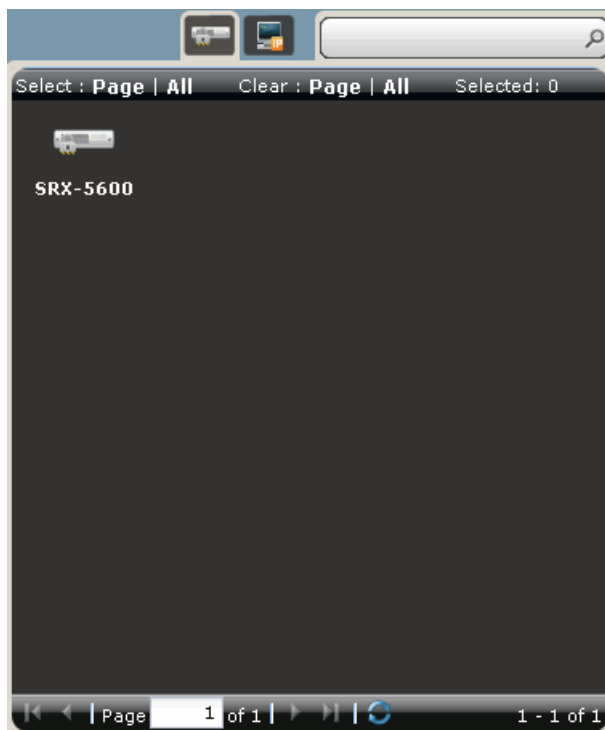
Dragging and Dropping Security Devices

To drag and drop 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 21 on page 52.

Figure 21: Device Chooser Panel



NOTE: Only security devices are shown in Device chooser.

2. From the Device chooser panel, drag and drop security devices to the Security Topology Whiteboard.

Connecting Security Devices

To connect security devices:

1. Click the Create Link icon on the toolbar and draw a line between security devices. This line represents the link between these security devices.

The link created between security devices is a logical link that may pass through other networking devices such as 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 Step 3 for the other end of the link and click **Configure**.



NOTE: The overlay icons indicate whether the device interfaces are configured. For example, a yellow triangle with a black exclamation point 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

To drag and drop 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 panel.
2. From the Address chooser panel, drag and drop addresses and address groups to the Security Topology Designer Whiteboard.



NOTE: You can use the Internet address object to define a topology that 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

To associate addresses with security devices:

1. Click the Create Link icon on 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 between a security device and an address is a logical link that may pass through other networking devices such as 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 that has a device.
4. Click **Configure**.

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

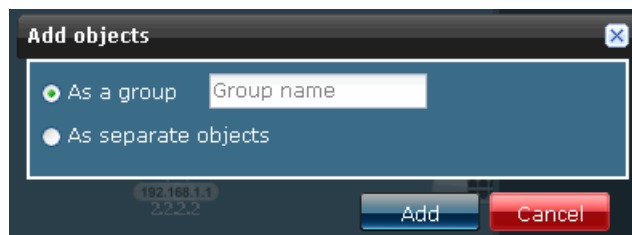
Creating Device Groups

To create device groups:

1. Select multiple devices from the Device chooser panel and drag and drop them to the Security Topology Designer Whiteboard.

The **Add Objects** window is displayed, as shown in Figure 22 on page 54.

Figure 22: Add Objects Window



2. In the **As a group** field, enter a name for the device group.
3. Click **Add**.

The device group is displayed on the Security Topology Designer 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 Security 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.

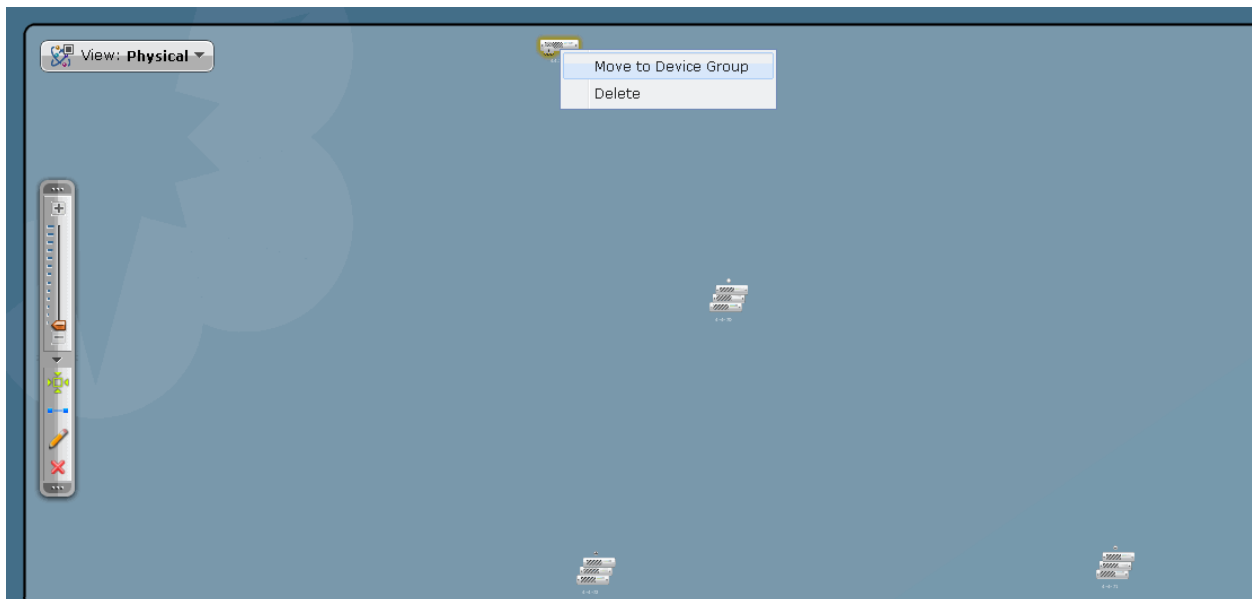
Moving Ungrouped Devices into a Device Group

To move an ungrouped device on the topology whiteboard to a device group:

1. Right-click the ungrouped device and select **Move to Device Group** from the contextual menu, as shown in Figure 23 on page 55.

The **Move to Device Group** popup window is displayed.

Figure 23: Adding Ungrouped Devices into a Group



2. From the **Device Group** drop-down menu, select the device group you want to move this device to.
3. Click **Move**.

The device is moved into the selected device group.

Removing Devices from a Device Group

To remove devices from a device group:

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

The device is removed from the device group.

Searching for Devices and Addresses in the Topology

To search for devices or addresses in the topology:

1. In the search field next to the object chooser icons, enter the name of the device or address you want to search for.
2. Click the magnifying glass icon next to the search field.

All devices or addresses that match the search criterion are highlighted on the Security Topology Designer Whiteboard.

If your search criteria corresponds to a device within a device group, the group hosting the object searched for expands and highlights the object.



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

Creating Group Links on Device Groups

To create group links on device groups:

1. Click the Create Link icon on the toolbar and draw a line between the device group and the device you want to link.

The interfaces that are shown in the device group are 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 are 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 that has a device.
4. Repeat Step 2 and Step 3 for the other end of the link and click **Configure**.

This link is displayed in a different color.



NOTE: You can view the number of individual links configured by placing the cursor on the link.

Adding Addresses and Security Domains Using CSV Import

To add addresses and security domains using CSV import:

1. Right-click the Security 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 with 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 in the **Select CSV File** window.

The fields available in the sample CSV file are as described in Table 4 on page 57

Table 4: Adding Addresses and Security Domains Using CSV Import

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



NOTE: You cannot upload address groups using the CSV import functionality. You can upload IP address, network, IP range and hostname.



NOTE: All devices that are associated with the addresses in the CSV file must already exist in the Device chooser panel.

Related Documentation

- Security Topology Overview on page 47
- Changing Topology Scapes on page 57

Changing Topology Scapes

To change the scape in the Security Topology Designer Whiteboard:

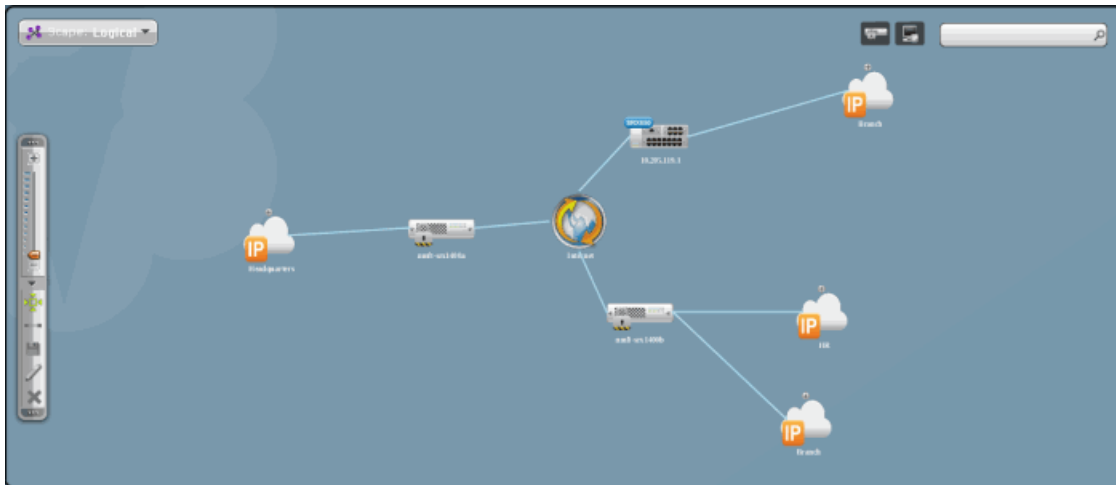
1. From the **Security Design** task ribbon, select **Security Whiteboard** > **Security Topology**.

The Security Topology Designer Whiteboard is displayed in the Physical scape.

2. From the scape selector on the top-left side of the whiteboard, select **Logical**.

The Logical scape of the topology is displayed, as shown in Figure 24 on page 58. You can view the device association with the security domains, based on the address associations with security domains.

Figure 24: Security Topology Designer Whiteboard: Logical Scape



- Related Documentation**
- Security Topology Overview on page 47
 - Creating a Security Topology on page 49

CHAPTER 9

Security Policies

- Security Policy Profiles Overview on page 59
- Creating Security Policy Profiles on page 61
- Managing Security Policy Profiles on page 64
- Security Policies Overview on page 66
- Creating Security Policies on page 68
- Deploying Security Policies on page 74
- Managing Security Policies on page 79
- Decommissioning Security Policies on page 83

Security Policy Profiles Overview

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

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

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

Junos Space provides two Juniper Networks defined policy profiles:

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
Documentation**

- [Creating Security Policy Profiles on page 61](#)
- [Managing Security Policy Profiles on page 64](#)

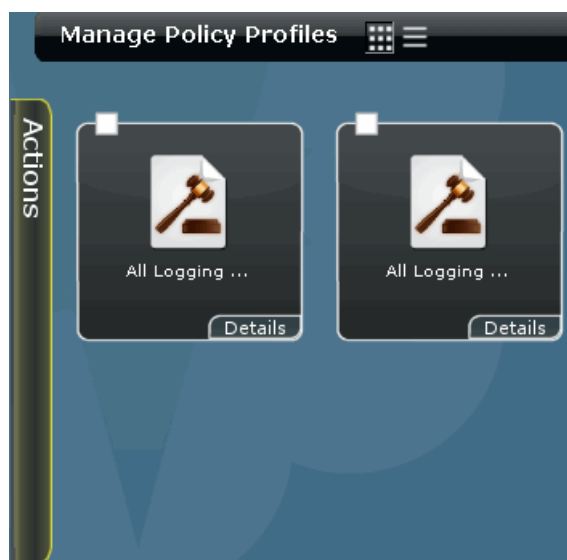
Creating Security Policy Profiles

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 25 on page 61. The first two policy profiles listed here are Juniper Networks defined policy profiles.

Figure 25: 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 26 on page 62.

Figure 26: 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. Use the **Logging** section of the **New Policy Profile** window to configure the log options for this policy profile. You can configure the following log options:
 - If you want to log the events when the session is created, select the **Log at Session Init** check box.
 - If you want to log the events when the session is closed, select the **Log at Session Close** check box.
 - If you want to enable counting, select the **Enable Count** check box.

If counting is enabled, counters are collected for the number of packets, bytes, and sessions that enter the firewall for a given policy
6. Use the **Firewall Authentication** section of the **New Policy Profile** window to provide authentication to clients, as shown in Figure 27 on page 63.

Figure 27: 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. Use the **Redirect** section of the **New Policy Profile** window to configure the traffic redirection options for this policy profile, as shown in Figure 28 on page 63:

Figure 28: New Policy Profile: Redirect Section

New Policy Profile

Name:

Description:

Logging Authentication Redirect

Redirect: ☒ None
☐ Redirect Wx
☐ Reverse Redirect Wx

Create Cancel

- If you want traffic to be redirected, select the **None** check box.

- If you want to enable Wx redirection for packets that arrive from the LAN, select the **Redirect Wx** check box.
- If you want to enable Wx redirection for the reverse flow of packets that arrive from the WAN, select the **Reverse Redirect Wx** check box.

8. Click **Create**.

The new security policy profile you have created is displayed in the **Manage Policy Profiles** inventory panel.

Related Documentation

- Security Policy Profiles Overview on page 59
- Managing Security Policy Profiles on page 64

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:

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

The **Manage Policy Profiles** inventory panel is displayed. All security policy policies created is listed by default, in the graphical view.

You can either right-click or use the Actions Drawer to manage a security policy profile. For more information about using the Actions Drawer, see [Inventory Pages Overview](#)

You can perform the following tasks in the **Manage Policy Profiles** space:

1. Viewing the Details of a Security Policy Profile on page 64
2. Modifying a Security Policy Profile on page 65
3. Copying a Security Policy Profile on page 65
4. Deleting a Security Policy Profile on page 66
5. Searching for a Security Policy on page 66

Viewing the Details of a Security Policy Profile

To view the details of a security policy profile:

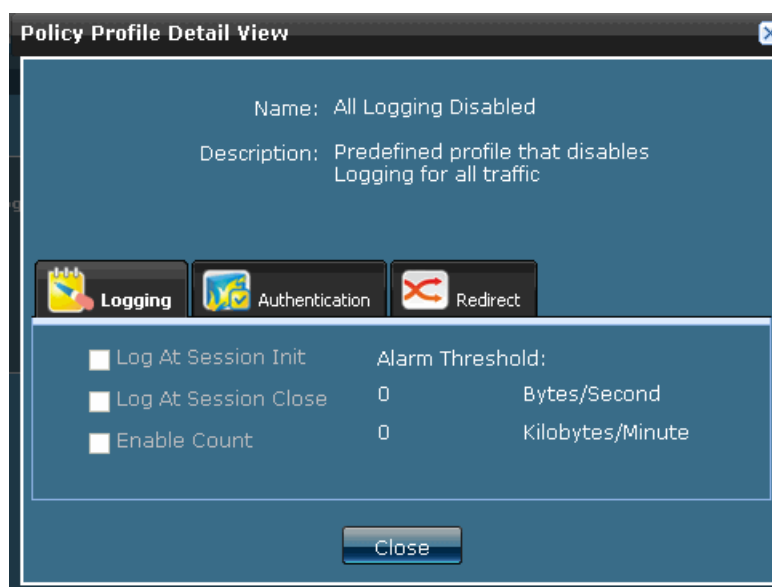
1. From the **Security Design** task ribbon, select **Security Whiteboard > Security Policy > Policy Profiles**.

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 29 on page 65.

Figure 29: Policy Profile Detail View Window



3. Click **Close**.

Modifying a Security Policy Profile

To modify a security policy profile you have created:

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

The **Manage Policy Profiles** inventory panel is displayed.

2. Right-click the security policy profile that 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**.

Copying a Security Policy Profile

To copy a security policy profile you have created:

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

The **Manage Policy Profiles** inventory panel is displayed.

2. Right-click the security policy profile that 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.

Deleting a Security Policy Profile

To delete a security policy profile you have created:

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

The **Manage Policy Profiles** inventory panel is displayed.

2. Right-click the security policy profile that 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**.

Searching for a Security Policy

To search for a security policy profile you have created:

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

The **Manage Policy Profiles** inventory panel is displayed.

2. In the **Search** field, enter the name of security policy profile you want to search.

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 Documentation**
- Security Policy Profiles Overview on page 59
 - Creating Security Policy Profiles on page 61

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. You can use security policies 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. You can also specify 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.

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.

In general, to configure a security policy using the Policy Designer Whiteboard:

1. Drag and drop the security domains that are the end points of a security policy.
2. Create a policy between the security domains that 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
Documentation**

- [Creating Security Policies on page 68](#)
- [Deploying Security Policies on page 74](#)
- [Managing Security Policies on page 79](#)
- [Decommissioning Security Policies on page 83](#)

Creating Security Policies

To create security policies between security domains:

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





The **Security Policy Designer Whiteboard** is displayed, as shown in Figure 30 on page 68.

Figure 30: Security Policy Designer Whiteboard



The toolbar on the left displays a set of functions you can perform to design security policies, as listed in Table 5 on page 68.

Table 5: Security Policy Designer Toolbar Icons

Toolbar Icon	Icon Name	Description
	Show All	Fit the policy graph on the Policy Designer Whiteboard
	Create Policy	Create a policy between security domains
	Save Coordinates	Save a security policy design
	Delete	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 and sub-domains are 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 31 on page 69.

Figure 31: Create Policy Window

Create Policy

Engg IP ——— IP HR

Name:

Description:

Profile: All Logging Enabled ▼

Rules

Direction	Applications	Action	Settings
↔	rtsp tftp tacacs-ds tacacs bootpc	⛔	
→	ftp netbios-session smtp	✅	
←	telnet ssh	✅	

Create Cancel

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. From the **Profile** field, select an appropriate policy profile.

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 in which the traffic flows
- Applications that are a part of the rule
- Whether traffic is permitted or denied in the given direction
- 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.

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

- To add a rule:

- a. Select the Add icon.

The **Add Rule** window is displayed, as shown in Figure 32 on page 71.

Figure 32: Add Rule Window



- b. In the **Description** field, enter an appropriate description.
- c. Select one or more applications from the **Available** section of the dialog box and click the Add icon.
The application you have selected are displayed in the **Selected** section of this dialog box.
- d. From the **Direction** section of the **Add Rule** window, select the direction of traffic.
- e. From the **Action** section of the **Add Rule** window, select the action to be performed on the traffic.
- f. To make any specific changes to the policy profile settings used in this rule, click **Advanced Setting**.

The **Rule Details** window displays the policy profile settings used for this rule.

- g. 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.

- h. 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.

- To delete a rule:
 - Select the rule you want to delete and click the **Delete** icon.
- To edit a rule:
 - a. Select the rule you want to edit and click the **Edit** icon.
The **Rule Details** window is displayed.
 - b. In the **Direction** section, make appropriate changes to the direction of traffic.
 - c. In the **Action** section, make appropriate changes to the action performed by the security policy.
 - d. To add more applications to this rule move the applications from the **Available** section to the **Selected** section.
 - e. To make any specific changes to the policy profile settings used in this rule, click **Advanced Setting**.
The **Rule Details** window displays the policy profile settings used for this security policy.
 - f. To ensure that the changes made to the policy profile settings in the **Rule Details** window affect only this rule, select the **Use Custom Settings for This Rule** check box.
 - g. Make appropriate changes to the policy profile settings and click **OK**.

The **Settings** column for 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:

- 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 74.

To delete a security policy:

- 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 79.



NOTE: You can clear a security policy design from the Policy Designer Whiteboard. You must first delete the security policy to be able to delete the security domains that are the end points of a security policy.

To clear a security policy design from the Policy Designer Whiteboard:

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 Documentation

- Security Policies Overview on page 66
- Deploying Security Policies on page 74
- Managing Security Policies on page 79
- Decommissioning Security Policies on page 83

Deploying Security Policies

To deploy or provision a security policy you have created:

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 that you want to provision and select **Provision Policy** from the contextual menu.

The **Provision Policy** window displays the devices on which this policy is provisioned. You can view the device name, device IP address, platform, Junos OS version, configuration state, connection status, and the XML commands, as shown in Figure 33 on page 74.

Figure 33: Provision Security Policy Window

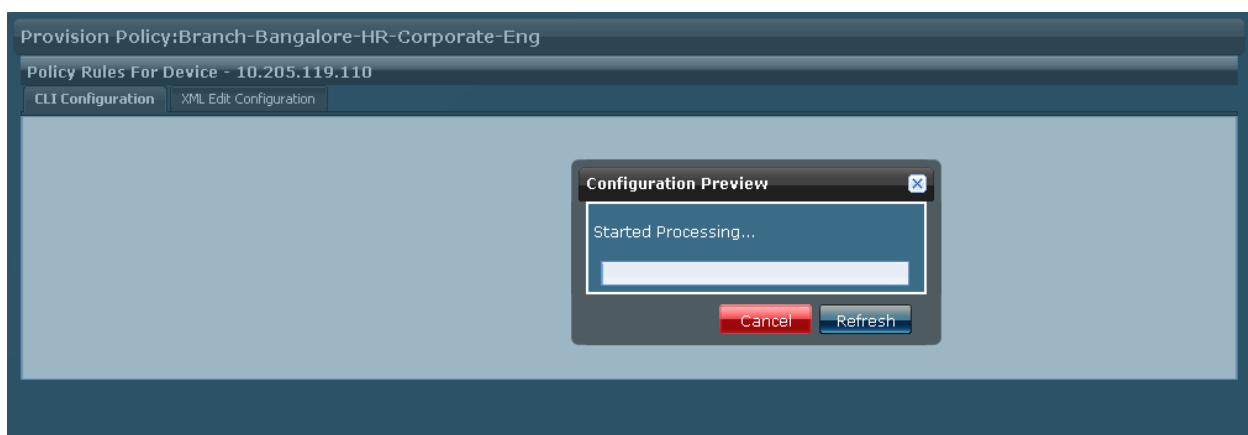
Provision Policy:HR-Finance							
Name	Device IP	Platform	OS Version	Configuration St	Managed Status	Connection Stat	Configuration
10.204.77.19	10.204.77.19	SSG550	6.3.0r1.0	New	In Sync	up	view
10.204.77.23	10.204.77.23	SSG20-WLAN	6.3.0as.0	Modify	In Sync	up	view

☐ Schedule at a later time

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

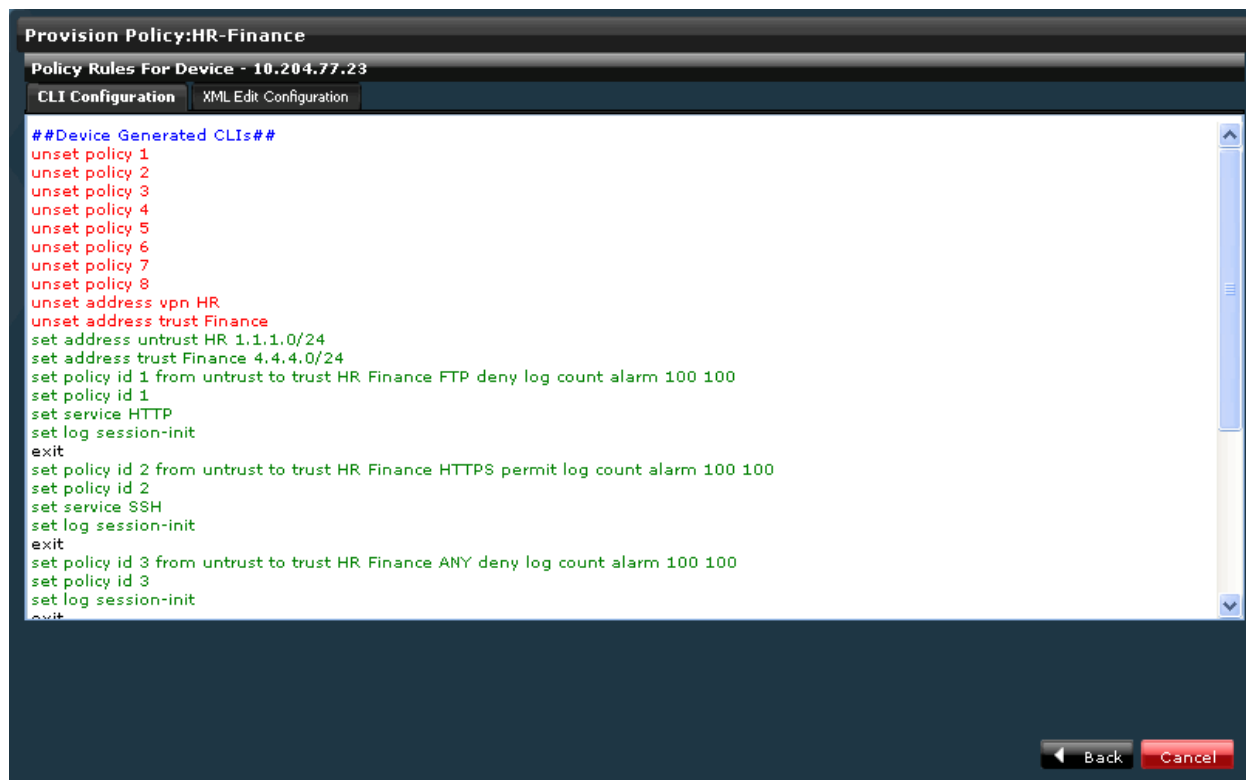
3. If you want to preview the configuration changes pushed to the device, click the **View** link in the **Configuration** column corresponding to the device. A **Configuration Preview** progress bar is shown while the configuration pushed to the device is generated, as shown in Figure 34 on page 74.

Figure 34: Configuration Preview



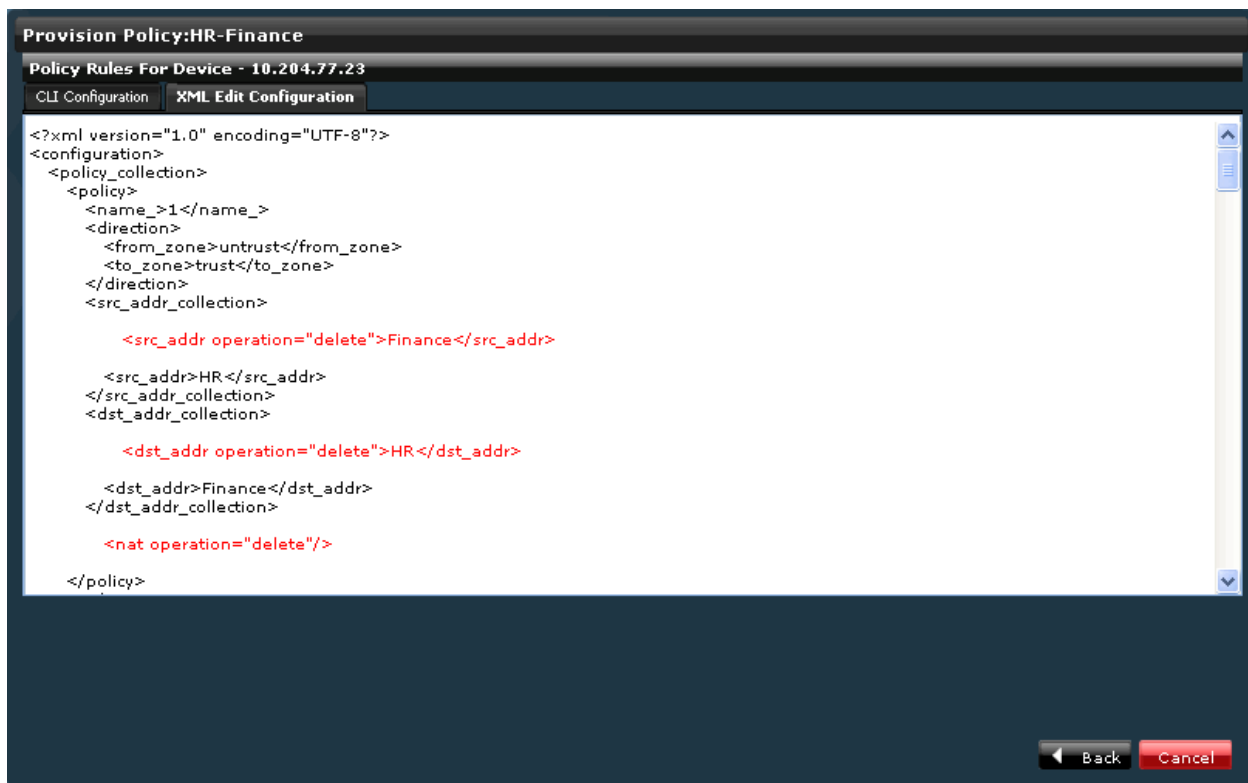
The **CLI Configuration** tab is displayed by default. You can view the configuration details, as shown in Figure 35 on page 75.

Figure 35: Viewing CLI Commands: Policy



4. To view the XML format of the configuration, click the **CLI Configuration** tab.
You can view the configuration details, as shown in Figure 36 on page 76.

Figure 36: View XML Commands: Policy



5. Select the check box next to the **Schedule Provisioning** field to schedule the provisioning to a later time and date.
6. Select appropriate values from the **Date and Time** fields.
7. Click **Provision**.

The security policy is provisioned on the devices that are a part of this policy. A new job is created and the job ID is displayed in the **Job Information** dialog box.

8. 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 security policy 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 messages 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 synchronized with Junos Space.
- Configuration Update Failed: This indicates configuration commit errors. This error message includes the error message sent by the device.

- No Interface Selected in topology: This indicates that the interface on which the address is connected is not selected when an address link is created to a device.
- Address not associated with any device in topology: This indicates that the address exists in a domain but is not associated with any device in the topology.

A security policy is placed in a specific state based on whether it is provisioned, not provisioned, or partially provisioned. An overlay icon is placed over the security policy icon to depict the different states. The different states that a security policy is placed in are shown in Table 6 on page 78.

Table 6: Security Policy Provision States

State	Overlay Icon
Provisioned	
Not Provisioned	
Partially Provisioned	



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 Step 3 through Step 6 to provision the security policy.



NOTE: If you try to provision a security policy and the provision job fails, the security policy is placed in the Not Provisioned state. It may also be placed in the Partially Provisioned state if the configuration is passed onto at least one device before the provisioning job failed. You can provision or delete this security policy using the appropriate workflow.



NOTE: When a security policy between two security domains is provisioned, the policy uses the paths defined by the IPsec VPN created between the security devices associated with the security domains.

**Related
Documentation**

- Security Policies Overview on page 66
- Creating Security Policies on page 68
- Managing Security Policies on page 79
- Decommissioning Security Policies on page 83

Managing Security Policies

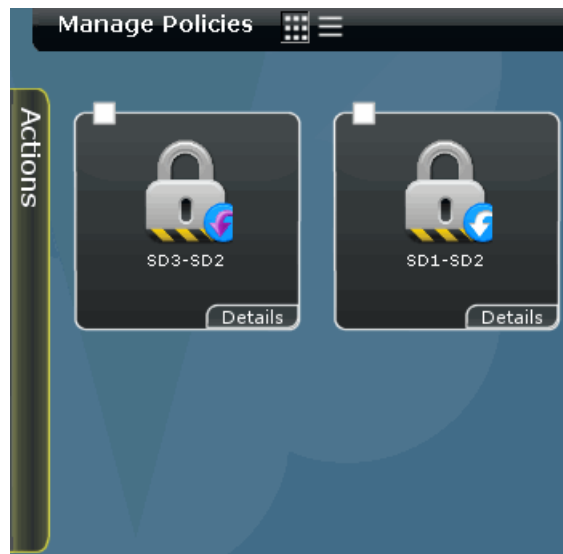
You can view, modify or delete security policies listed in the **Manage Policies** inventory panel.

To open the **Manage Policies** inventory panel:

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

The **Manage Policies** inventory panel is displayed, as shown in Figure 37 on page 80. All security policies created are listed by default, in the tabular view.

Figure 37: Manage Policies Inventory Panel



You can either right-click or use the Actions Drawer to manage a security policy. For more information about using the Actions Drawer, see [Inventory Pages Overview](#)

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

1. Viewing the Details of a Security Policy on page 80
2. Modifying a Security Policy on page 81
3. Deleting a Security Policy on page 81
4. Searching for a Security Policy on page 81
5. Viewing Job Details on page 81

Viewing the Details of a Security Policy

To view the details of a security policy you have created:

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:

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**.

Deleting a Security Policy

To delete a security policy you have created:

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**.

Searching for a Security Policy

To search for a security policy you have created:

1. From the **Security Design** task ribbon, select **Security Whiteboard > Security Policy**.
The **Manage Policies** inventory panel is displayed
2. In the **Search** field, enter the name of security policy you want to search.
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.

Viewing Job Details

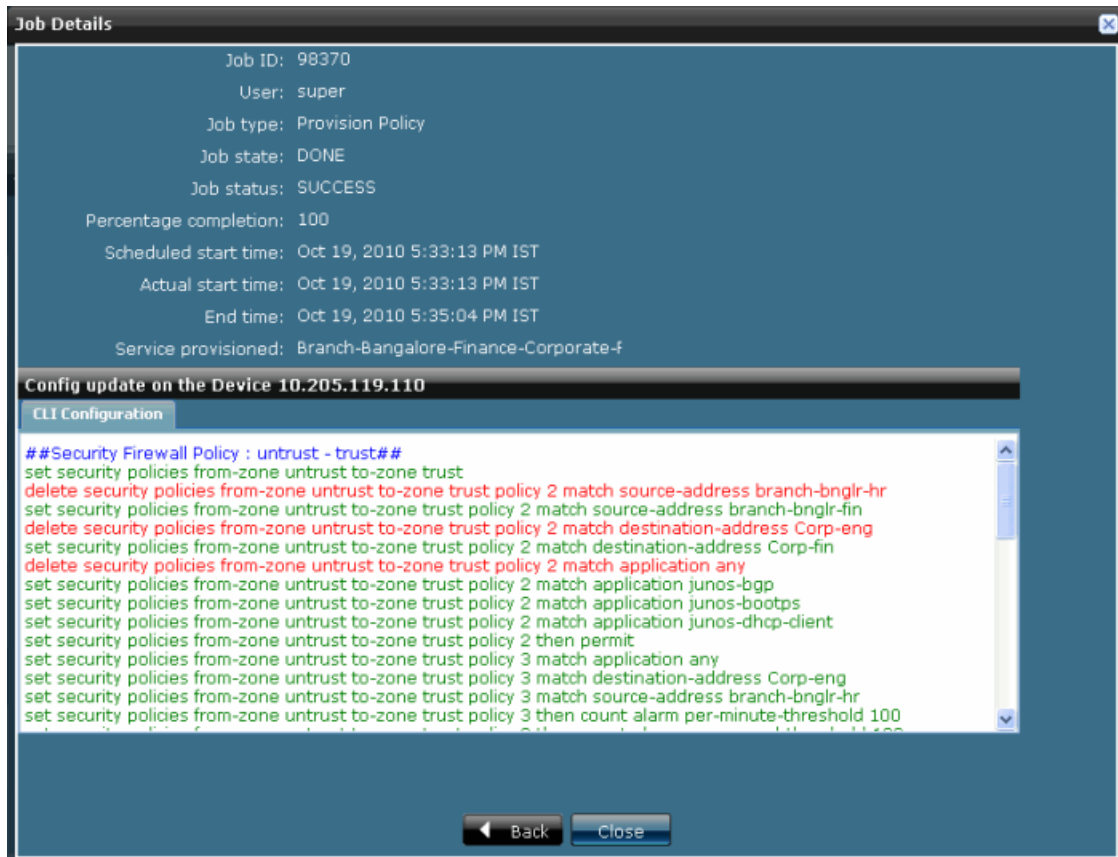
To view the job details of the policy that is provisioned:

1. From the **Security Design** task ribbon, select **Job Management > Manage Jobs**.
The **Manage Jobs** inventory panel is displayed
2. Double-click the security policy whose job details you want to view.
The **Job Details** window is displayed.

3. In the **Device Provisioning Details** section, click the **View** link corresponding to the device.

The CLI format of the configuration pushed to the device is displayed, as shown in Figure 38 on page 82.

Figure 38: Job Details Window



- Related Documentation**
- Security Policies Overview on page 66
 - Creating Security Policies on page 68
 - Deploying Security Policies on page 74
 - Decommissioning Security Policies on page 83

Decommissioning Security Policies

To decommission a security policy you have provisioned:

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 you want to decommission and select **Decommission Policy** from the contextual menu.

The **Decommission Policy** window displays the devices on which this security policy is provisioned, as shown in Figure 39 on page 83.

Figure 39: Decommissioning a Security Policy

Name	Device IP	Platform	OS Version	Connection Status	XML Commands
10.205.61.61	10.205.61.61	SRX210H	10.2R1.4	down	view
10.205.61.62	10.205.61.62	SRX210H	10.2R1.4	down	view

Page 1 of 1

☒ Delete service after job succeeds

☒ Schedule at a later time

Date and Time: 07/07/10 1:54 PM IST

Decommission Cancel

3. To automatically delete the security policy from Junos Space after the security policy is decommissioned, select the **Delete service after job succeeds** check box.
4. To schedule the decommissioning to a later time and date, select the check box next to the **Schedule at a later time** field.
5. Click **Next**.
6. Select appropriate values from the **Date and Time** fields.
7. Click **Decommission**.



NOTE: If a provision job on a security policy partially succeeds, (that is, the provision job does not push the configuration details to all devices in the security policy), the security policy is placed in the Partially Provisioned state. You can provision or decommission the security policy using the appropriate workflow.



NOTE: If you try to delete a security policy that is in the Provisioned state, a popup window confirming whether you want to decommission the security policy is displayed. You can click Yes to decommission the security policy before deleting it or click No to delete the security policy without decommissioning it.

**Related
Documentation**

- Security Policies Overview on page 66
- Creating Security Policies on page 68
- Managing Security Policies on page 79
- Deploying Security Policies on page 74

CHAPTER 10

NAT

- NAT Overview on page 85
- Creating a NAT Policy on page 87
- Provisioning a NAT Policy on page 95
- Decommissioning a NAT Policy on page 97
- Managing NAT Policies on page 98
- Managing NAT Pools on page 100

NAT Overview

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

NAT is usually configured on gateway devices such as SRX Series Services Gateways and ScreenOS devices in order to translate traffic between the trust and untrust zones. Whenever a packet comes to the NAT device, the device performs a translation on the packet's IP address by rewriting it with an IP address that was specified for external use. After translation, the packet appears to have originated from the gateway rather than from the original device within the network. This helps you hide internal IP addresses from the other networks and keep your network secure.

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

Junos Space supports two types of NAT:

- Source NAT: Translates the source IP address of a packet leaving the trust zone (outbound traffic). It translates the traffic originating from one side of the network (only source). Using source NAT, an internal device can access the network by using the IP addresses specified in the NAT policy.
- Static NAT: Always translates a private IP address to the same public IP address. It translates traffic from both sides of the network (both source and destination). For

example, a web server with a private IP address can access to the Internet using a static, one-to-one address translation.

Junos Space Security Design provides you with a workflow where you can create and provision NAT policies on devices in a network.

There are three main steps in configuring NAT on a device:

a. Define a NAT pool.

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

For more information about defining a NAT pool, see “Managing NAT Pools” on page 100.

b. Define a NAT policy.

A NAT policy is a collection of rules that defines how the device should translate addresses.

You use NAT rules to specify conditions that the traffic must match in order for address translation to take place. When a packet matching the criteria specified in a NAT rule arrives, the device translates the address of the packet according to the specified rules. The address can be translated to a constant IP address range or to a range of IP addresses picked randomly from an address pool.

NAT policies also maintain information about the devices to which the NAT policies were applied.

For more information about defining a NAT policy, see “Creating a NAT Policy” on page 87.

c. Provision the NAT policy to the device.

For more information about provisioning a NAT policy, see “Managing NAT Policies” on page 98.

To go to the NAT task:

1. From the application chooser, click **Security Design**.
The **Security Design** dashboard appears.
2. From the Security Design task ribbon, select **Security Whiteboard > NAT**.
The **Manage NAT Policies** page appears (Figure 40 on page 86).

Figure 40: Manage NAT Policies Page

Name	Description	End Point 1	End Point 2	Devices	Deployment Status
test		1.1.1.1	2.2.2.2	4.4.80.1	Not Provisioned

Here you can perform the following actions:

- Create a NAT policy
- Modify a NAT policy
- Delete a NAT policy
- Provision a NAT policy
- Decommission a NAT policy

**Related
Documentation**

- [Creating a NAT Policy on page 87](#)
- [Provisioning a NAT Policy on page 95](#)
- [Decommissioning a NAT Policy on page 97](#)
- [Managing NAT Policies on page 98](#)
- [Managing NAT Pools on page 100](#)

Creating a NAT Policy

A NAT policy is a collection of rules that defines how a device should translate addresses.

To create a NAT policy:

1. From the Security Design task ribbon, select **Security Whiteboard > NAT > Create NAT Policy**.

The **Create NAT Policy** page appears (Figure 41 on page 88).

Figure 41: Create NAT Policy Page

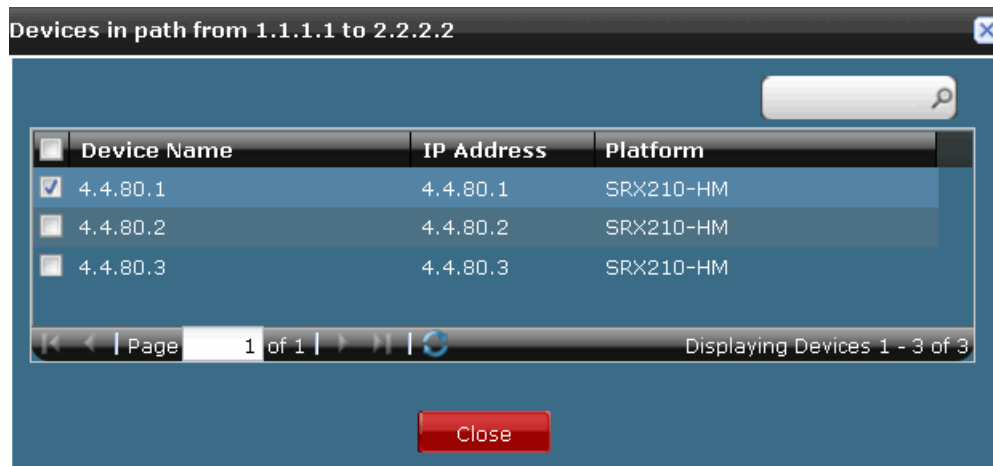
2. Enter a name for the NAT policy in the **Policy Name** field.
3. Enter a description for the NAT policy in the **Description** field. This is optional.
4. Select either **Any address**, **IP address/Subnet**, or **Domain Name** and enter the appropriate values of the traffic endpoints in the fields provided.



NOTE: Security Design interprets an empty traffic endpoint field as **Any address**. While you can choose to enter the details of only one of the endpoints, you cannot leave both fields empty.

5. Click **Search Devices** to search for all devices that lie between the two specified endpoints.
The Device list dialog box appears displaying the devices according to name and IP address. (Figure 42 on page 89)

Figure 42: List of Devices Between the Specified Endpoints



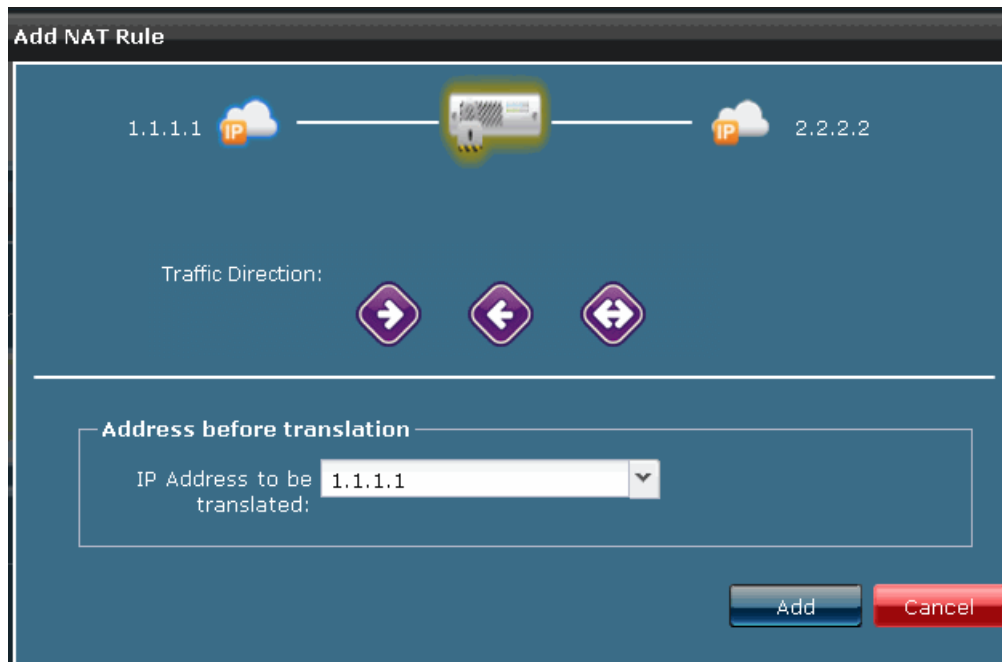
6. Select the devices on which you want to apply the NAT policy.
7. Click **Close** to close the dialog box and return to the **Create NAT Policy** page. The selected devices are displayed in the cloud and a new table called **NAT Rules** is displayed at the bottom of the page. The **NAT Rules** table (Figure 43 on page 89) displays all the NAT rules according to the original IP address, traffic direction, translated IP address, and whether port translation is enabled.

Figure 43: NAT Rules

Original IP	Direction	Translated IP	Port Translation
2.2.2.2	→	Interface	✓

8. Click the **Add** button to open the **Add NAT Rule** dialog box. (Figure 44 on page 90)

Figure 44: Add NAT Rule Dialog Box



The dialog box is titled "Add NAT Rule". It features a diagram at the top showing a router icon with two IP addresses, 1.1.1.1 and 2.2.2.2, connected by a line. Below the diagram, the "Traffic Direction:" section contains three buttons: a right-pointing arrow, a left-pointing arrow, and a double-headed arrow. A horizontal line separates this from the "Address before translation" section, which contains a text field labeled "IP Address to be translated:" with the value "1.1.1.1" and a dropdown arrow. At the bottom right, there are "Add" and "Cancel" buttons.

9. Here you can perform the following actions:

- Create a Source NAT Rule. See “Create a Source NAT Rule” on page 90.
- Create a Static NAT Rule. See “Create a Static NAT Rule” on page 93.

10. After you have specified all the NAT rules for the NAT policy, click **Create** to save the NAT policy.

The **Manage NAT Policies** page appears displaying the newly created NAT policy.



NOTE: You can also modify or delete NAT rules.

To modify a NAT rule, select the NAT rule and click the **Modify** button. Make the appropriate changes in the **Modify NAT Rule** dialog box.

To delete a NAT rule, select the NAT rule and click the **Delete** button. This removes the rule from the list.

Create a Source NAT Rule

To create a source NAT rule:

1. In the **Create Rule** dialog box, enter the IP address that you want to translate in the **IP Address to be translated** field.
2. Select the unidirectional arrow button to make the selected endpoint the source. The **Translation panel** appears (Figure 45 on page 91).

Figure 45: Add Source NAT Rule

Add NAT Rule

1.1.1.1 — — 2.2.2.2

Traffic Direction:

Address before translation

IP Address to be translated:

Translation Parameters

☒ Interface
 ☐ IP/Subnet
 ☐ NAT Pool

☒ Port Translation

3. Here, you can select one of the following options:

- **Interface:** Select **Interface** if you want the original address to be translated to the IP address of the egress interface. Source port addresses are translated by default. When port translation is used, multiple hosts can share the same IP address.
- **IP/Subnet:** Select **IP/Subnet** if you want the original address to be translated to a specific IP address (Figure 46 on page 92), and specify the following details:
 - Select the egress interface that is bound to the untrust zone from the **Egress interface** list.



NOTE: For Screen OS devices, the **Egress interface** list displays all the egress interfaces. You need to select an egress interface and configure the pool.

For SRX devices, you can select the **All** option if you want to configure a common pool for all the interfaces. You can also select one egress interface and configure the pool.

- Enter the IP address that the address must translate to in the **IP/Subnet** field.
- Select the **Port Translation** check box to enable Port Address Translation (PAT) which uses the source address of the port to identify the devices.

Figure 46: Translation Parameters for IP/Subnet Option

The screenshot shows a dialog box titled "Translation Parameters" with a dark blue background. At the top, there are three radio buttons: "Interface", "IP/Subnet" (which is selected), and "NAT Pool". Below the radio buttons, there is a label "Egress Interface:" followed by a dropdown menu showing "All". Underneath that is a label "IP/Subnet:" followed by a text input field. At the bottom left, there is a checkbox labeled "Port Translation" which is currently unchecked. At the bottom right, there are three buttons: "Advance Settings" (with a right-pointing arrow), "Add" (in blue), and "Cancel" (in red).

- **NAT Pool:** Select **NAT Pool** if you want the original address to be translated to an address in the NAT pool (Figure 47 on page 92).
 - Select the egress interface that is bound to the untrust zone from the **Egress interface** list.
 - Select the NAT pool from the list. You can also click **Create New** to open the **Create NAT Pool** dialog box where you can create a new NAT pool.
 - Select the **Port Translation** check box to enable network Port Address Translation (PAT) which uses the source address of the port to identify the devices.

Figure 47: Translation Parameters for NAT Pool Option

The screenshot shows a dialog box titled "Translation Parameters" with a dark blue background. At the top, there are three radio buttons: "Interface", "IP/Subnet", and "NAT Pool" (which is selected). Below the radio buttons, there is a label "Egress Interface:" followed by a dropdown menu showing "Please select...". Underneath that is a label "NAT Pool:" followed by a text input field showing "Select/create a pool". To the right of this field are two small icons: a magnifying glass and a green plus sign. At the bottom left, there is a checkbox labeled "Port Translation" which is currently unchecked. At the bottom right, there are three buttons: "Advance Settings" (with a right-pointing arrow), "Add" (in blue), and "Cancel" (in red).

- Click **Advanced...** to open the **Advanced Options-Source NAT** dialog box (Figure 48 on page 93).

This option is not enabled if you select **Interface**.

Figure 48: Advanced Settings

- In the **Advanced Options-Source NAT** dialog box, enter the host address base in the **Host Address Base** field. The host address base is the starting address in the range specified in the NAT pool.
For example, suppose you have configured a pool whose range is 1.1.1.1 through 1.1.1.10. If you have specified 1.1.1.5 as the host address base, only addresses from 1.1.1.5 through 1.1.1.10 are used for translation.
- Select a NAT pool from the **Overflow Pool** list to specify a pool of addresses that can be used for translation if all the addresses in the original NAT pool are used up. You can enable port translation if you do not want to specify an overflow pool. Port translation conserves the addresses in the pool by using their port addresses for translation.
- Enter the destination address of the packet in the **Destination Address** field. The source address of the packet is translated only if the destination address in its header matches this address.
- Click **Add** to save your settings and return to the **Create Rule** dialog box.
- Click **OK** to save the NAT rule.
The **Create NAT Policy** page appears displaying the new NAT rule in the **NAT Rule** table.

Create a Static NAT Rule

To create a static NAT rule:

- In the **Create Rule** dialog box, enter the IP address that you want to translate in the **IP Address to be translated** field.
- Select the bidirectional arrow option.
The **Translation Panel** appears (Figure 49 on page 94).

Figure 49: Add Static NAT Rule

Add NAT Rule

1.1.1.1 — — 2.2.2.2

Traffic Direction:

☒ ☐

Address before translation

IP Address to be translated:

Translation Parameters

☒ IP/Subnet

Ingress Interface:

IP/Subnet:

3. Select the ingress interface that the IP addresses must be translated to from the **Ingress Interface** list.



NOTE: For Screen OS devices, the **Ingress Interface** list displays all the ingress interfaces. You need to select an ingress interface and configure the pool.

For SRX devices, you can select the All option if you want to configure a common pool for all the interfaces. You can also select one ingress interface and configure the pool.

4. Enter the IP address that you want the original address to always be translated to in the **IP/Subnet** field.
5. Click **Add** to save the NAT rule.

The **Create NAT Policy** page appears displaying the new NAT rule in the **NAT Rule** table.

- Related Documentation**
- NAT Overview on page 85
 - Provisioning a NAT Policy on page 95
 - Decommissioning a NAT Policy on page 97
 - Managing NAT Policies on page 98
 - Managing NAT Pools on page 100

Provisioning a NAT Policy

To deploy or provision a NAT policy:

1. From the Security Design task ribbon, select **Security Whiteboard > NAT** . The **Manage NAT Policies** page appears.
2. Select the NAT policy that you want to provision and click **Provision NAT Policy** from the **Actions** panel or from the right-click context menu.

The **Provision NAT** page appears (Figure 50 on page 95), displaying the devices on which this policy can be provisioned as described in Table 7 on page 96.

Figure 50: Provision NAT Policy

Provision NAT:test1

Name	Device IP	Platform	OS Versi	Config Sta	Managed St	Connection St	Configuration
10.205.35.1	10.205.35.1	SSG550	6.2.0r2.0	New	In Sync	up	View

Affected Services

Service Name	Service Type	Details
L1-R1	Security Policy	View

☐ Schedule at a later time

[Provision](#) [Cancel](#)

The **Affected Services** panel displays all other policies that are affected when you provision the NAT policy. The services are displayed according to service name and type (VPN or firewall), and provides you with a link to view the details of the affected service. You must reprovision these services so that they are no longer affected by the NAT policy.

3. Click **Provision** to provision the NAT policy on the specified devices.

You can also choose to schedule the provisioning job for later. To do so, select **Schedule at a later time** and select the date and time from the lists.



NOTE: Whenever you provision a NAT policy, it affects the other provisioned security policies (such as firewalls and VPN policies) existing on the device. You must reprovision these services so that they are no longer affected by the provisioned NAT policy.

When you reprovision a firewall policy, Security Design modifies the list of permitted addresses in the firewall policy according to the existing NAT policies and adds the modifications to the existing policy. It does not delete any part of the original policy.

For example, a firewall policy that permits traffic originating from the IP address “1.1.1.1” contains the “permit 1.1.1.1” statement. When a packet whose source address “1.1.1.1” is translated to “2.2.2.2” arrives at the firewall device, it may not be granted access. In order to overcome this, you must reprovision the firewall policy. When you reprovision the policy, Security Design adds the “permit 2.2.2.2” statement to the policy and provisions it.

When you reprovision a VPN policy, Security Design modifies the route that forwards VPN traffic to the tunnel interface to reflect the translated address. It replaces the original source address with the translated address.

For example, if the source address is translated from 1.1.1.1 to 2.2.2.2, the destination address of the route that the packet takes when it returns to the source is changed from 1.1.1.1 to 2.2.2.2. This new rule is added to the existing policy. None of the rules existing in the original policy are removed.

Table 7: Provision NAT Policy Table Descriptions

Column Name	Description
Name	Name of the device
Device IP	IP address of the device
Platform	Device model. For example: SRX240-HM.
OS Version	Release version of the Junos OS running on the device
Configuration Status	Status of the device configuration. The possible options are New and Modified .

Table 7: Provision NAT Policy Table Descriptions (*continued*)

Column Name	Description
Managed Status	<p>Status of the devices that are managed in Junos Space.</p> <p>The possible options are:</p> <ul style="list-style-type: none"> • Connecting • In Sync • None • Out of Sync • Synchronizing • Sync Failed
Connection Status	Status of the Connection of the device in Junos Space. The possible options are Up or Down .
Configuration View	Click View to see the device configuration.

- Related Documentation**
- NAT Overview on page 85
 - Creating a NAT Policy on page 87
 - Managing NAT Policies on page 98
 - Decommissioning a NAT Policy on page 97

Decommissioning a NAT Policy

To decommission a NAT policy:

1. From the Security Design task ribbon, select **Security Whiteboard > NAT** .
The **Manage NAT Policies** page appears.
2. Select the NAT policy that you want to provision and click **Decommission NAT Policy** from the **Actions** panel or from the right-click context menu.
The **Decommission NAT** page appears (Figure 51 on page 98) displaying the devices on which this policy is provisioned.

Figure 51: Decommission NAT Policy

Name	Device IP	Platform	OS Versio	Config Sta	Managed St	Connection Sta	Config
10.205.35.100	10.205.35.100	SSG550	6.2.0r2.0	Modify	In Sync	up	View

☐ Delete service after job succeeds

☐ Schedule at a later time

[Decommission](#) [Cancel](#)

3. Select the **Delete service after job succeeds** option to automatically delete the NAT policy from Junos Space after the NAT policy is decommissioned.
4. Click **Decommission** to remove the NAT policy from the device.

Related Documentation

- NAT Overview on page 85
- Creating a NAT Policy on page 87
- Provisioning a NAT Policy on page 95
- Managing NAT Policies on page 98

Managing NAT Policies

A NAT policy is a collection of rules that defines how the device should translate addresses.

You use NAT rules to specify conditions that the traffic must match in order for address translation to take place. When a packet matches the criteria specified in a NAT rule, the device translates the source address of the packet according to the rules that you have specified.

In case of source NAT, the source address of the packet is translated either to the IP address of the interface with port translation, to a subnet, or to a pool of IP addresses. This translation occurs only on traffic originating at one side of the network (usually the trust zone) and the translation is dynamic. There is no one-to-one relationship between the original and translated addresses.

In case of static NAT, translation occurs on traffic originating at both sides of the network (both the trust and untrust zones). There is a one-to-one relationship between the original and translated addresses.

You can perform the following tasks in the Manage NAT Policies page:

- Modifying a NAT Policy on page 99
- Deleting a NAT Policy on page 99

Modifying a NAT Policy

To modify a NAT policy:

1. From the Security Design task ribbon, select **Security Whiteboard > NAT**. The **Manage NAT Policies** page appears.
2. Select the NAT policy that you want to modify and click **Modify NAT Policy** from the Actions panel or from the right-click context menu. The **Modify Policy** window is displayed.
3. Make appropriate changes to the NAT policy. You can modify all the fields in this window, except the **Name** field.
4. Click **Modify** to save your changes and go back to the **Manage NAT Policies** page.



NOTE: When you modify a NAT policy that has already been provisioned, you need to provision the policy again in order for the changes to be reflected on the device. For information about how to provision a NAT policy, see “Provisioning a NAT Policy” on page 95.

Deleting a NAT Policy

To remove a NAT policy from Junos Space:

1. From the Security Design task ribbon, select **Security Whiteboard > NAT**. The **Manage NAT Policies** page appears.
2. Select the NAT policies that you want to delete and click **Delete NAT Policy** from the Actions panel or from the right-click context menu. The **Delete NAT Policy** dialog box appears listing out all the NAT policies that you have selected.
3. Click **Delete** to remove the NAT policy from Junos Space. If you try to delete a provisioned policy, a message appears asking whether you want to decommission the policy on the device. For information about how to decommission a NAT policy, see “Decommissioning a NAT Policy” on page 97.

Related Documentation

- NAT Overview on page 85
- Creating a NAT Policy on page 87
- Provisioning a NAT Policy on page 95
- Decommissioning a NAT Policy on page 97
- Managing NAT Pools on page 100

Managing NAT Pools

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

Using Security Design, you can create and manage NAT pools, which you can use while creating NAT policies.

The tasks that you can perform in the **Manage NAT Pools** space include:

- Creating a NAT Pool on page 100
- Modifying a NAT Pool on page 101
- Deleting a NAT Pool on page 101

Creating a NAT Pool

To create a NAT pool:

1. From the Security Design task ribbon, select **Security Whiteboard > NAT > Manage NAT Pool > Create NAT Pool**.

The **Create NAT Pool** page appears (Figure 52 on page 100).

Figure 52: Create NAT Pool Page

2. Enter the name of the NAT pool in the **Name** field.
3. Enter a description of the NAT pool in the **Description** field.
4. Enter the range of IP addresses in the **Start IP address** and **End IP address** fields. You can specify a range of up to 2000 IP addresses.



NOTE: While you can enter single IP addresses or subnets in the **Start IP Address** and **End IP Address** fields, you cannot enter both a subnet and a single IP address within the same range.

5. Click **Create** to save your changes and go back to the **Manage NAT Pools** page where the newly created NAT pool is displayed.

Modifying a NAT Pool

To modify a NAT Pool:

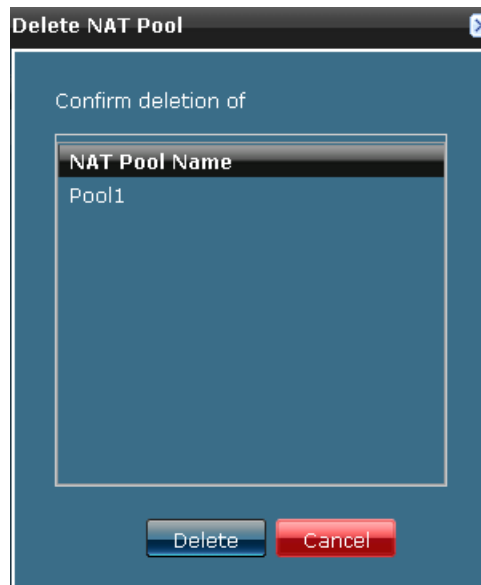
1. From the Security Design task ribbon, select **Security Whiteboard > NAT > Manage NAT Pool**.
The **Manage NAT Pool** page appears.
2. Select the NAT pool that you want to modify and click **Modify NAT Pool** from the **Actions** panel or from the right-click context menu.
The **Modify NAT Pool** page appears.
3. On the **Modify NAT Pool** page, you can edit the description and IP range of the NAT pool. You cannot modify the NAT pool name.
4. Click **Modify** to save your changes and go back to the **Manage NAT Pool** page.
Security Design warns you when you try to modify a NAT pool used in a NAT policy.

Deleting a NAT Pool

To delete a NAT pool:

1. From the Security Design task ribbon, select **Security Whiteboard > NAT > Manage NAT Pool**.
The **Manage NAT Pool** page appears.
2. Select the NAT pool that you want to delete and click **Delete NAT Pool** from the **Actions** panel or from the right-click context menu.
The **Delete NAT Pool** page appears displaying all the NAT pools that you want to delete (Figure 53 on page 102).

Figure 53: Delete NAT Pool Dialog Box



3. Click **Delete** to remove the NAT pool from the list and go back to the **Manage NAT Pool** page.
Security Design warns you when you try to delete a NAT pool used in a NAT policy.

**Related
Documentation**

- NAT Overview on page 85
- Creating a NAT Policy on page 87
- Managing NAT Policies on page 98

CHAPTER 11

IPsec VPNs

- VPN Proposals Overview on page 103
- Creating VPN Proposals on page 104
- Managing VPN Proposals on page 108
- VPN Profiles Overview on page 112
- Creating VPN Profiles on page 112
- Managing VPN Profiles on page 118
- IPsec VPNs Overview on page 123
- Creating IPsec VPNs on page 123
- Deploying IPsec VPNs on page 127
- Managing IPsec VPNs on page 133
- Decommissioning IPsec VPNs on page 135

VPN Proposals Overview

You can use the 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 Security Associations (SAs). An IPsec proposal exchanges information between established IPsec SAs through an IPsec tunnel.

You can 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. You can use this to create VPN profiles.

Junos Space provides three Juniper Networks defined VPN proposals. The parameters of these VPN proposals are listed in Table 8 on page 104.

Table 8: 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 Documentation**
- Creating VPN Proposals on page 104
 - Managing VPN Proposals on page 108

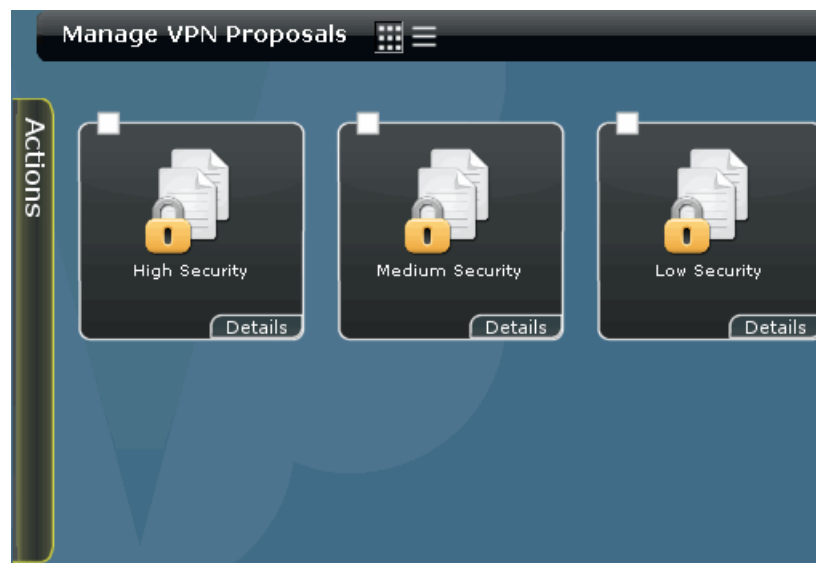
Creating VPN Proposals

To create a new VPN proposal:

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 54 on page 104. The first three proposals listed here are Juniper Networks defined VPN proposals.

Figure 54: 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 55 on page 105.

Figure 55: Create VPN Proposal Window

The screenshot shows the 'Create VPN Proposal' window. It features a title bar at the top. Below the title bar, there are two text input fields: 'Name:' and 'Description:'. Underneath these fields are two panels. The first panel is titled 'IKE Proposals (maximum 4)' and contains a large empty rectangular area. To the right of this area are three icons: a green plus sign, a pencil, and a red X. The second panel is titled 'IPSec Proposals (maximum 4)' and also contains a large empty rectangular area with the same three icons to its right. At the bottom of the window, there are two buttons: 'Create' and 'Cancel'.

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. You can either add a predefined proposal or a custom proposal in the **IKE Proposal** dialog box.

6. To add a predefined IKE proposal:
 - a. Select the **Predefined** radio button.
 - b. From the **Name** field, select an appropriate proposal

To add a custom IKE proposal:

- a. Select the **Custom** radio button, as shown in Figure 56 on page 106.

Figure 56: Adding a Custom IKE Proposal

The screenshot shows the 'IKE Proposal' dialog box. It has two radio buttons: 'Predefined' and 'Custom'. The 'Custom' radio button is selected. Below the radio buttons are five fields: 'Name' (a text input field), '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 input field showing '3600'). At the bottom of the dialog 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** drop-down menu, select an appropriate group
- d. From the **Authentication** drop-down menu, select an appropriate authentication algorithm.
- e. From the **Encryption** drop-down menu, 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.

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

- a. Select the **Custom** radio button, as shown in Figure 57 on page 107.

Figure 57: 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 fields and dropdown menus: 'Name' (a text input field), 'DH Group' (a dropdown menu with 'Please select ...'), 'Authentication' (a dropdown menu with 'SHA-1'), 'Protocol' (a dropdown menu with 'Please select ...'), 'Encryption' (a dropdown menu with '3DES'), 'Life Time (in seconds)' (a text input field with '28800'), and 'Life Size (in KBs)' (a text input field). 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** drop-down menu, select an appropriate group.
- d. From the **Authentication** drop-down menu, select an appropriate authentication algorithm.
- e. From the **Encryption** drop-down menu, select an appropriate encryption standard.
- f. In the **Life Time (in seconds)** field, enter a value in seconds.
- g. In the **Life Size (in KBs)** field, enter a value in Kilo Bytes.



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

11. Click **Add**. Repeat Steps 10 through Step13 to add a maximum of four proposals.
- The proposals you have added are displayed in the **IPsec Proposals** panel.
12. Click **Create**.
- The new proposal you have created is displayed in the **Manage VPN Proposals** inventory panel.

- Related Documentation**
- VPN Proposals Overview on page 103
 - Managing VPN Proposals on page 108

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 that you have created are listed by default, in the graphical view.

You can either right-click or use the Actions Drawer to manage a VPN proposal. For more information about using the Actions Drawer, see Inventory Pages Overview

You can perform the following tasks in the **Manage VPN Proposals** space:

1. Viewing the Details of a VPN Proposal on page 108
2. Modifying a VPN Proposal on page 109
3. Deleting a VPN Proposal on page 110
4. Copying a VPN Proposal on page 111
5. Searching for a VPN Proposal on page 111

Viewing the Details of a VPN Proposal

To view the details of a VPN proposal:

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 Proposal Details** window, as shown in Figure 58 on page 109. The **VPN Proposal Details** window lists all the IKE and IPsec proposals used in this VPN proposal.

Figure 58: 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-sha	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-sh	Predefined	Group5	SHA-1	AES(128)	3600	ESP	0

Close

Modifying a VPN Proposal

To modify a VPN proposal you have created:

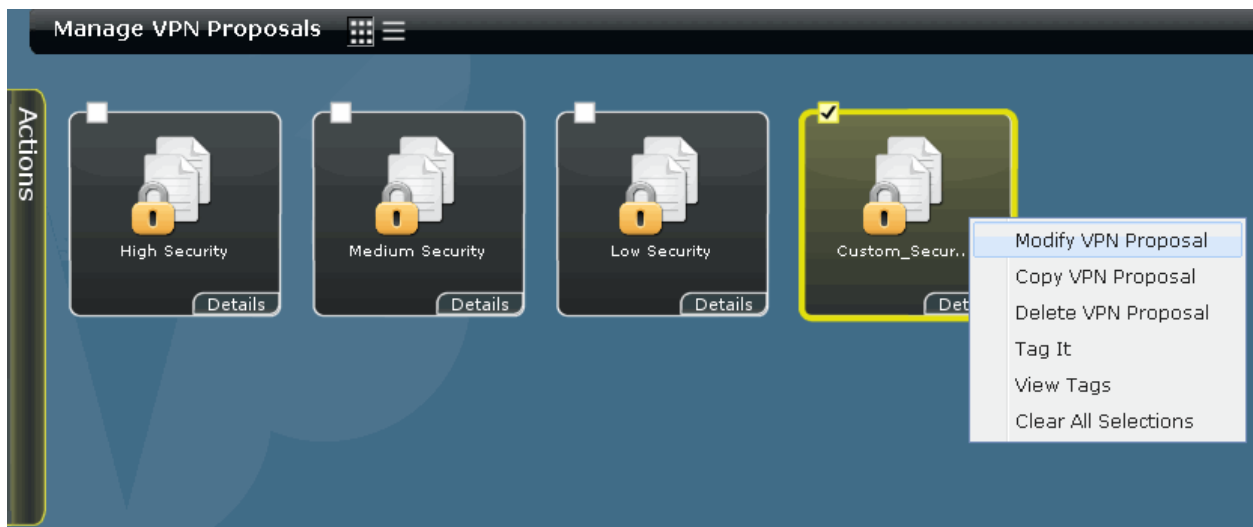
1. From the **Security Design** task ribbon, select **Security Whiteboard > IPsec VPN > VPN Proposal**.

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 59 on page 110.

This action redirects 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 59: Modifying a VPN Proposal



3. In the **Description** field, enter a new description.
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.

Deleting a VPN Proposal

To delete a VPN proposal you have created:

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 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 profile, you must first dis-associate the VPN proposal from the VPN profile.

Copying a VPN Proposal

To copy a VPN proposal you have created:

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 redirects 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

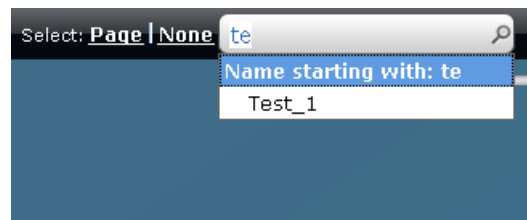
To search for a VPN proposal you have created:

1. From the **Security Design** task ribbon, select **Security Whiteboard > IPsec VPN > VPN Proposal**.

The **Manage VPN Proposals** inventory panel is displayed.

2. In the **Search** field, enter the name of VPN proposal you want to search, as shown in Figure 60 on page 111.

Figure 60: Searching for a VPN Proposal



3. Click the magnifying glass icon next to the **Search** field.

The **Manage VPN Proposals** inventory panel is populated with the VPN proposals matching your search criterion.

- Related Documentation**
- VPN Proposals Overview on page 103
 - Creating VPN Proposals on page 104

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.

You can 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. You can use this object to create route-based IPsec VPNs.

Junos Space provides two Juniper Networks defined VPN profiles:

- Site-To-Site – This profile is 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 – This profile is 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 Documentation**
- Creating VPN Profiles on page 112
 - Managing VPN Profiles on page 118

Creating VPN Profiles

To create a new VPN Profile:

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 61 on page 113. The first two profiles listed here are Juniper Networks defined VPN profiles.

Figure 61: 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 62 on page 113.

Figure 62: Creating a VPN Profile

The screenshot shows the "General" panel of the "Create VPN Profile" window. It has two main sections: "General" and "VPN Proposal". The "General" section contains fields for "Name:", "Type: Route Based", and "Description:". The "VPN Proposal" section has "Proposal Type:" with radio buttons for "Predefined" (selected) and "Custom". Below this is a "Predefined Proposals:" slider ranging from "High" to "Low", with the slider positioned at "High". At the bottom are four buttons: "Back", "Next", "Finish", and "Cancel".

In general, creating a VPN profile involves the following tasks:

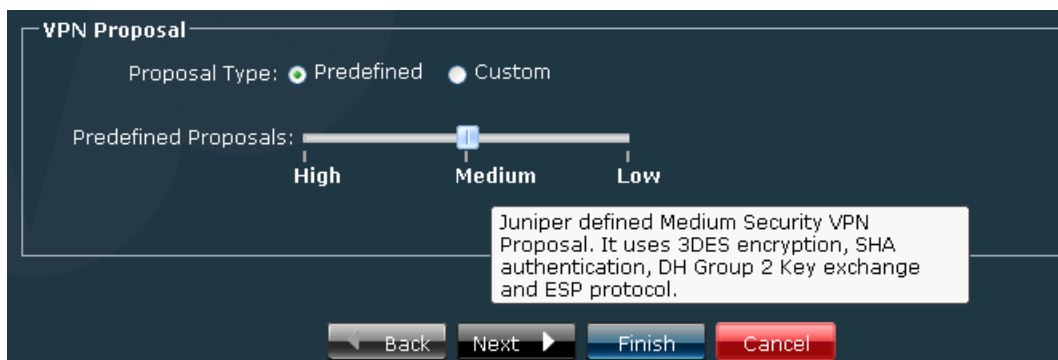
- Specifying the general settings
- Specifying the IKE/IPsec settings
- Specifying the connectivity parameters

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 63 on page 114. Mouse over on 'High', 'Medium' and 'Low' markers to view a tool tip description about the respective predefined proposal.

Figure 63: Choosing a Default VPN Proposal



- 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 is displayed. 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, as shown in Figure 64 on page 115.

Figure 64: Choosing a Custom VPN Proposal

VPN Proposal

Proposal Type: ☐ Predefined ☒ Custom

Custom Proposals: ▼ Add New Proposal

- e. If you want to add a new VPN proposal, click **Add New Proposal**.

This redirects you to the VPN Proposal creation page. For more information about creating a VPN proposal, see “Creating VPN Proposals” on page 104.

3. Click **Next**.

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 65 on page 115.

Figure 65: 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

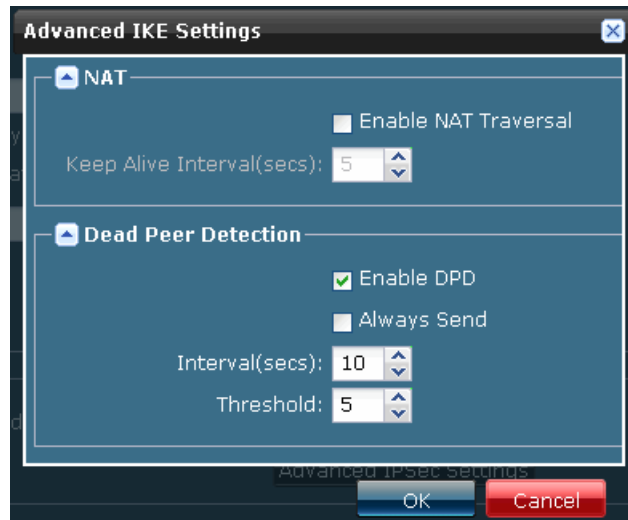
Advanced IPSec Settings

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 66 on page 116.

Figure 66: 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 in seconds.

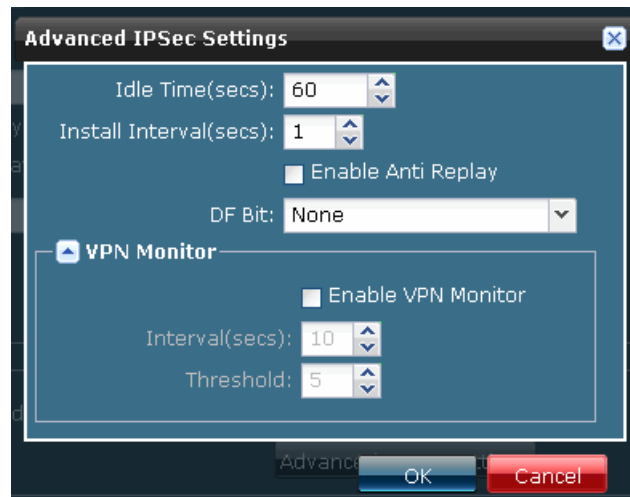
You can also increase or decrease the value currently displayed by selecting the upward or downward pointing arrows respectively.
7. Click **OK**.

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 67 on page 117.

Figure 67: 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 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**.
9. Click **Next**.

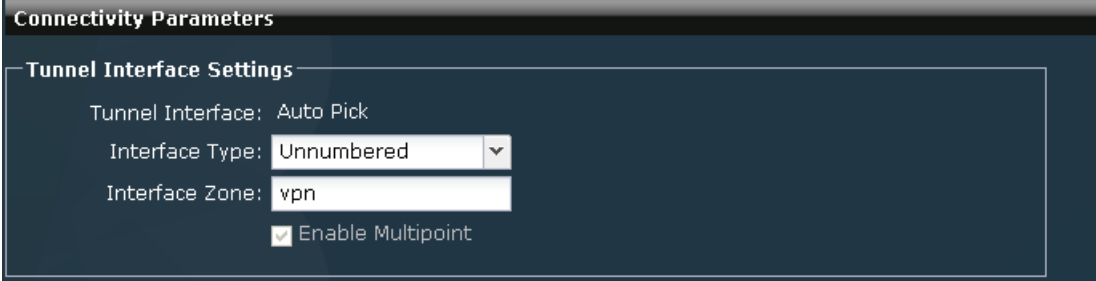
The **Connectivity Parameters** panel of the **Create VPN Profile** window is displayed.

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 68 on page 118.

Figure 68: Specifying Connectivity Parameters

The screenshot shows a window titled "Connectivity Parameters". Inside, there is a section titled "Tunnel Interface Settings". Within this section, there are three fields: "Tunnel Interface:" with the value "Auto Pick", "Interface Type:" with a dropdown menu showing "Unnumbered", and "Interface Zone:" with a text box containing "vpn". Below these fields is a checkbox labeled "Enable Multipoint" which is checked.

- 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**.

- Related Documentation**
- VPN Profiles Overview on page 112
 - Managing VPN Profiles on page 118

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.

You can either right-click or use the Actions Drawer to manage a VPN profile. For more information about using the Actions Drawer, see *Inventory Pages Overview*

You can perform the following tasks in the **Manage VPN Profiles** space:

1. Viewing the Details of a VPN Profile on page 119
2. Modifying a VPN Profile on page 120
3. Deleting a VPN Profile on page 121
4. Copying a VPN Profile on page 122
5. Searching for a VPN Profile on page 122

Viewing the Details of a VPN Profile

To view the details of a VPN profile:

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 69 on page 120.

The **VPN Profile Settings** window lists all the parameters you have specified for this profile.

Figure 69: Viewing the Details of a VPN Profile

The screenshot shows a window titled "VPN Profile Settings" with a close button in the top right corner. The window contains four expandable sections: "General Settings", "IKE Settings", "IPSec Settings", and "Tunnel Settings". The "General Settings" section is expanded and shows the following fields: "Name" with the value "VPN_Profile1", "Type" with the value "Route Based", "Description" (empty), and "VPN Proposal" with the value "Medium Security". The "Tunnel Settings" section is also expanded and shows: "Tunnel Interface" with the value "Auto Pick", "Tunnel Interface Type" with the value "UNNUMBERED", "Tunnel Interface Zone" with the value "vpn", and a checked checkbox for "Enable MultiPoint". A "Close" button is located at the bottom center of the window.

Modifying a VPN Profile

To modify a VPN profile you have created:

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 70 on page 121.

This action redirects 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 70: Modifying a VPN Profile



3. In the **Description** field, enter a new description
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**.

Deleting a VPN Profile

To delete a VPN profile you have created:

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**.

Copying a VPN Profile

To copy a VPN profile you have created:

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 **Copy VPN Profile** link from the contextual menu.

This action redirects 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

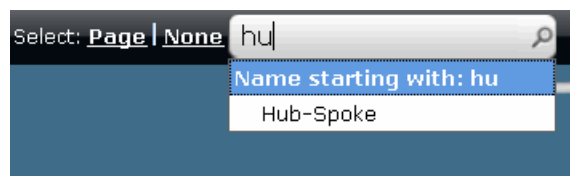
To search for a VPN profile you have created:

1. From the **Security Design** task ribbon, select **Security Whiteboard > IPsec VPN > VPN Profile**.

The **Manage VPN Profiles** inventory panel is displayed.

2. In the **Search** field, enter the name of VPN profile you want to search, as shown in Figure 71 on page 122.

Figure 71: Searching for a VPN Profile



3. Click the magnifying glass icon next to the **Search** field.

The **Manage VPN Profiles** inventory panel is populated with the VPN profiles matching your search criterion.

- Related Documentation**
- VPN Profiles Overview on page 112
 - Creating VPN Profiles on page 112

IPsec VPNs Overview

You can use an IPsec VPN Creation Wizard to create Site-To-Site and Hub-And-Spoke VPNs. The security topology you have created will serve as a base to create an IPsec VPN. You must configure the following 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

You can use the VPN Creation Wizard 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. After the configuration is saved, you can provision this VPN on the security devices.

- Related Documentation**
- Creating IPsec VPNs on page 123
 - Managing IPsec VPNs on page 133
 - Deploying IPsec VPNs on page 127
 - Decommissioning IPsec VPNs on page 135

Creating IPsec VPNs

To create an IPsec VPN:

1. 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.

2. 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 72 on page 124.


Figure 72: Create IPsec VPN:General Panel

General


Name:

Description:

VPN Type:




Site To Site




Hub And Spoke

Select Profile:

Site-To-Site

 Site-To-Site

 Hub-Spoke

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 type of VPN 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 unique tunnel IP range for every 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 125
2. Hub-And-Spoke on page 126

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.

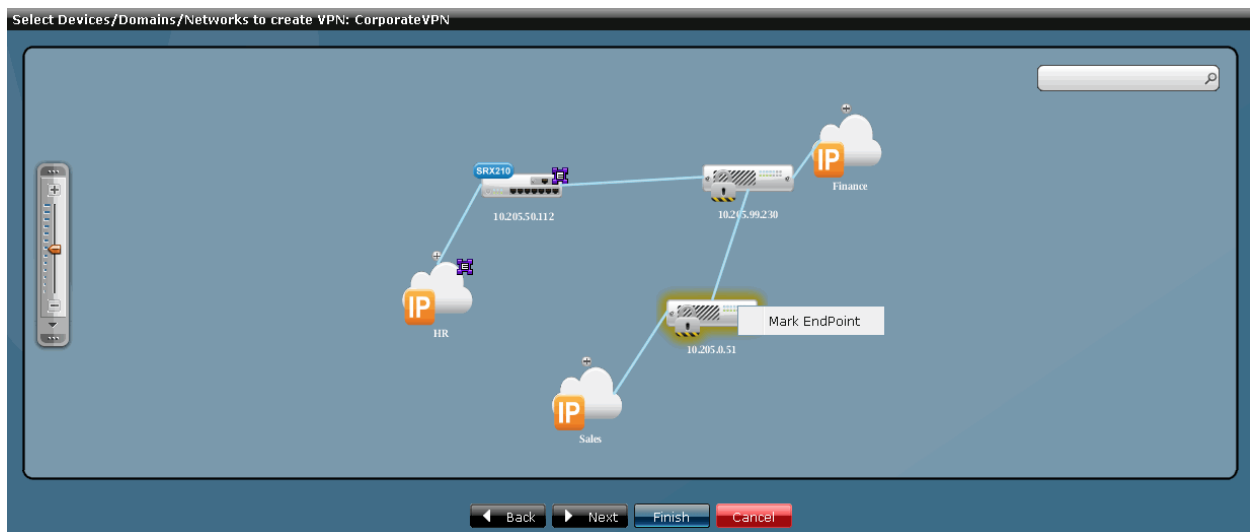
The new VPN you have created is displayed in the **Manage VPNs** inventory panel.

Hub-And-Spoke

To create a Hub-And-Spoke IPsec VPN:

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 73 on page 126.

Figure 73: 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 a 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.

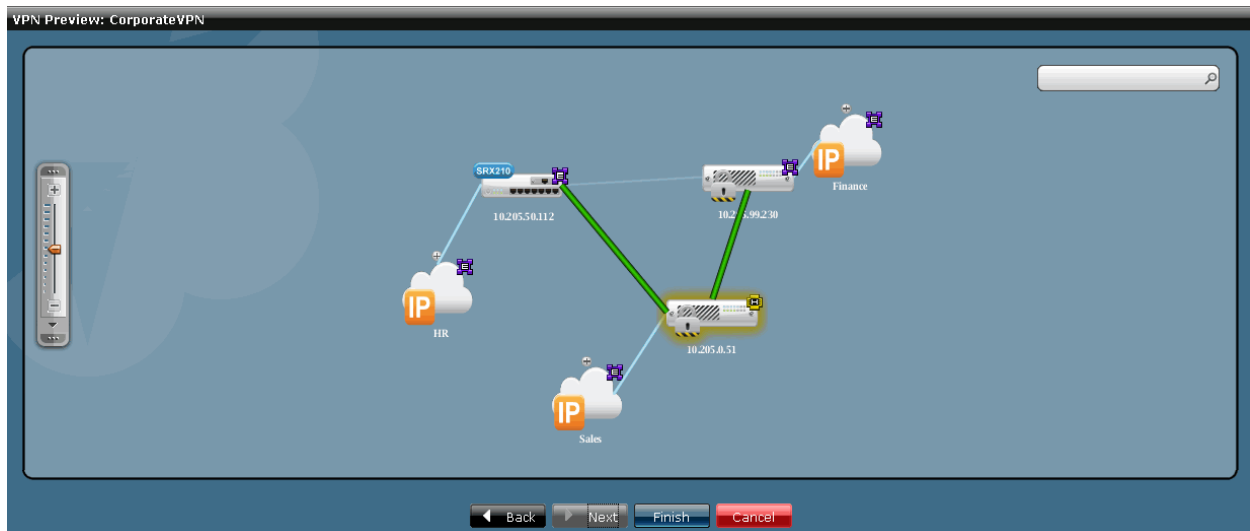
2. Right-click the device or the network that is the second spoke of the VPN and select **Mark Endpoint** from the contextual menu.
3. Right-click the device or the network that is the third spoke of the VPN and select **Mark Endpoint** from the contextual menu.
4. Right-click the spoke that you intend 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.

5. 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 74 on page 127.

Figure 74: VPN Overlay Over Topology



6. Click **Finish**.

The new VPN you have created is displayed in the **Manage VPNs** inventory panel.

Related Documentation

- IPsec VPNs Overview on page 123
- Managing IPsec VPNs on page 133
- Deploying IPsec VPNs on page 127
- Decommissioning IPsec VPNs on page 135

Deploying IPsec VPNs

To deploy or provision an IPsec VPN that you have created:

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 that 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 address, platform, Junos OS version, configuration state, connection status, and the XML commands, as shown in Figure 75 on page 128.

Figure 75: Provision VPN Window

Provision VPN:CorporateVPN							
Name	Device IP	Platform	OS Version	Configuration St	Managed Status	Connection Stat	Configuration
10.205.50.112	10.205.50.112	SRX210-HM	10.0R3.10	New	In Sync	up	view
10.205.0.51	10.205.0.51	SSG140	6.3.0r4.0	New	In Sync	up	view
10.205.99.230[Intermediate]	10.205.99.230	NSISG1000	6.3.0r1.0	New	In Sync	up	view

☐ ☒ Schedule at a later time _____

[Provision](#) [Cancel](#)

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

- 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. The **XML Edit Configuration** tab is displayed by default. You can view the configuration details, as shown in Figure 76 on page 128.

Figure 76: View XML Commands:VPN

Provision VPN:test

VPN configuration for device - 10.205.119.1

CLI Configuration XML Edit Configuration

```

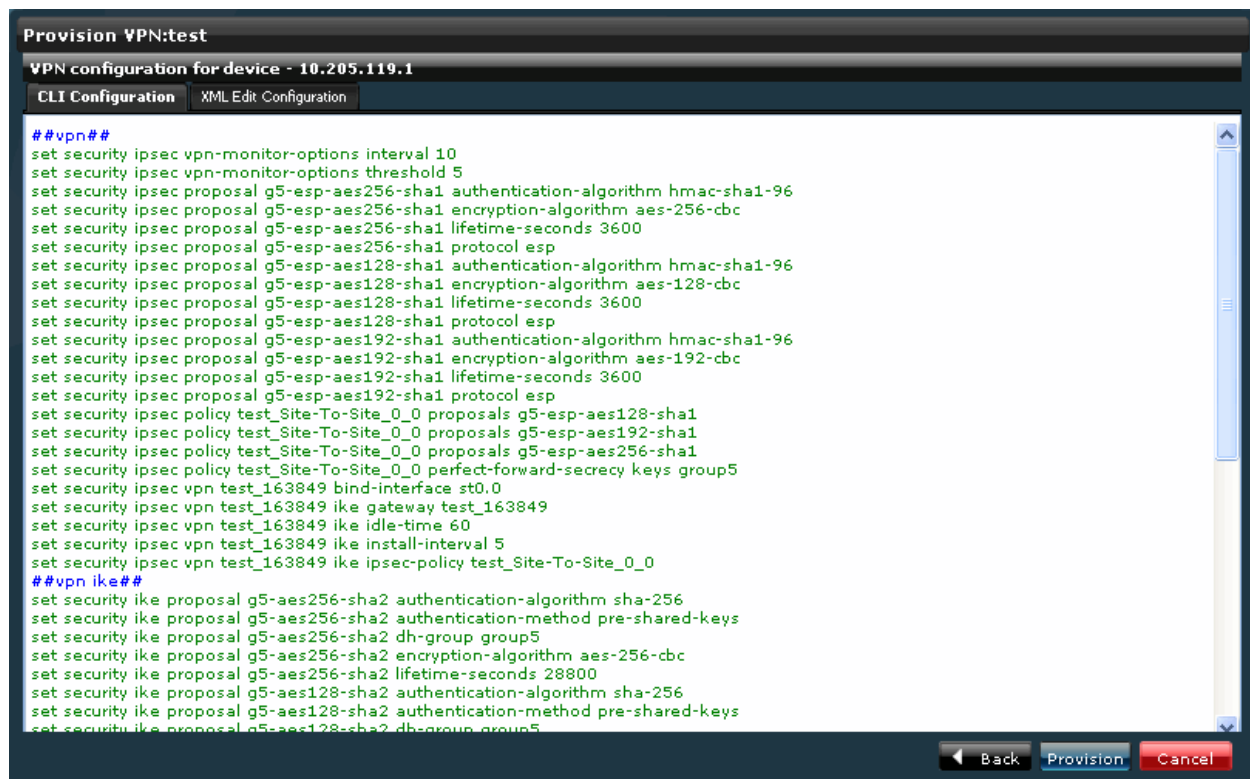
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
  <interfaces>
    <interface operation="create">
      <name>st0</name>
      <unit>
        <name>0</name>
        <family>
          <inet/>
        </family>
      </unit>
    </interface>
  </interfaces>
  <routing-options>
    <static>
      <route operation="create">
        <name>2.2.2.2/32</name>
        <next-hop>st0.0</next-hop>
      </route>
    </static>
  </routing-options>
  <security>
    <ike>
      <proposal operation="create">
        <name>g5-aes256-sha2</name>
        <authentication-algorithm>sha-256</authentication-algorithm>
        <authentication-method>pre-shared-keys</authentication-method>
        <dh-group>group5</dh-group>
      </proposal>
    </ike>
  </security>
</configuration>

```

[Back](#) [Provision](#) [Cancel](#)

- If you want to view the CLI configuration details, click the **CLI Configuration** tab. You can view the configuration details, as shown in Figure 77 on page 129.

Figure 77: Viewing CLI Commands: VPN



5. Select the check box next to the **Schedule Provisioning** field to schedule the provisioning to a later time and date.
6. Select appropriate values from the **Date and Time** fields.
7. Click **Provision**.

The IPsec VPN is provisioned on the devices that are a part of this VPN. A new job is created and the job ID is displayed in the **Job Information** dialog box.

8. 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 messages 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 synchronized 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. Click **Provision**.

An IPsec VPN is placed in a specific state based on whether it is provisioned, not provisioned, or partially provisioned. An overlay icon is placed over the IPsec VPN icon to depict the different states. The different states that an IPsec VPN is placed in is listed in Table 9 on page 131.

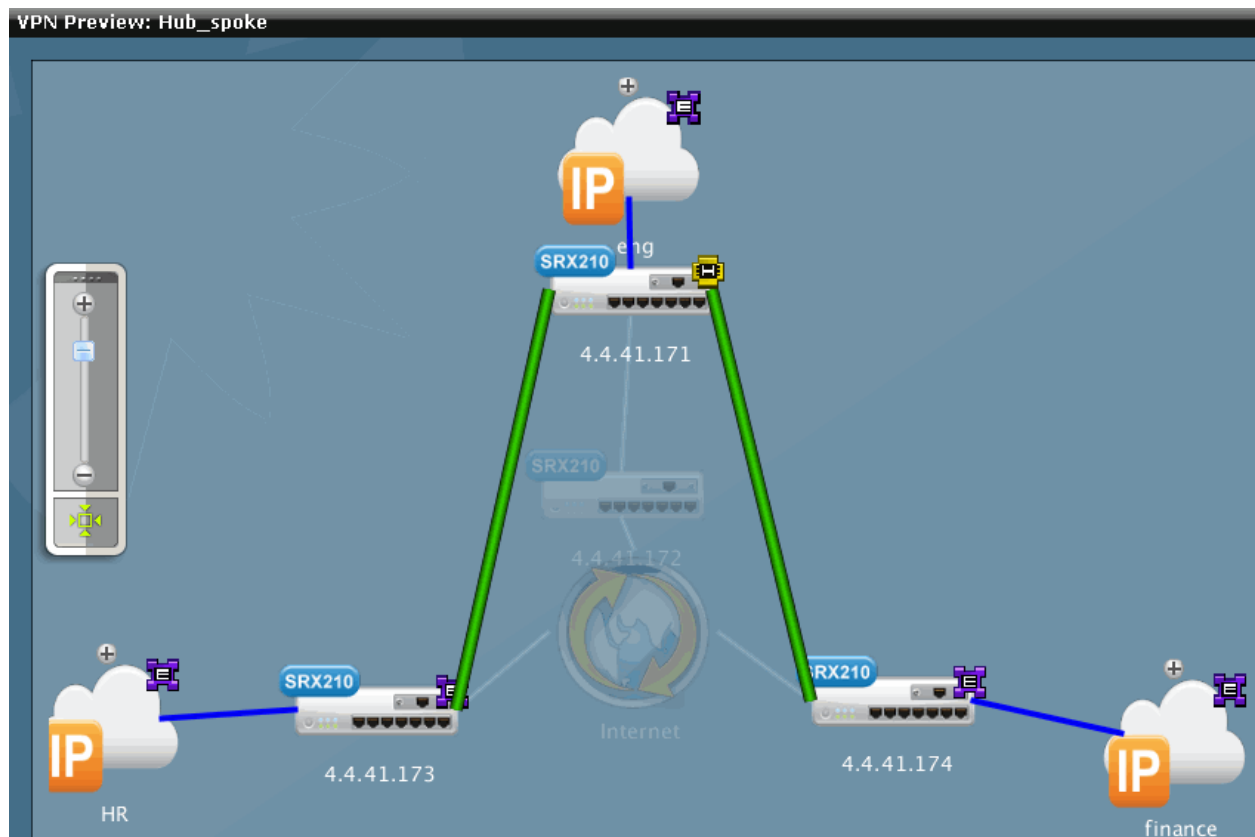
Table 9: IPsec VPN Provision States

State	Overlay Icon
Provisioned	 The icon shows a dark square with a small white square in the top-left corner. Inside, there's a green line connecting two nodes, a yellow padlock, and a blue circular arrow. The word "site" is at the bottom, and a "Details" button is in the bottom-right corner.
Not Provisioned	 The icon is similar to the Provisioned state but features a blue lightning bolt instead of a circular arrow. The word "new" is at the bottom, and a "Details" button is in the bottom-right corner.
Partially Provisioned	 The icon shows a green line connecting two nodes with a cross, a yellow padlock, and a blue circular arrow. The word "hub" is at the bottom, and a "Details" button is in the bottom-right corner.



NOTE: If you are provisioning a VPN which has an intermediate firewall, Junos Space automatically configures the intermediate firewall with the policy to allow the IKE/IPsec traffic for VPN. The Provision VPN window lists the intermediate device along with the VPN endpoints. You can preview the configuration sent to the intermediate device. You can view a typical VPN configuration which leads to the policy creation in Figure 78 on page 132.

Figure 78: IPSec VPN with an Intermediate Firewall





NOTE: When you provision a VPN, you can view all security policies that are impacted, as shown in Figure 79 on page 133.

Figure 79: Policies Affected While Provisioning a VPN

Provision VPN: MyHnSVpn							
Name	Device IP	Platform	OS Version	Configuration Sta	Managed Status	Connection Statu	Configuration
10.205.119.1[Intermediate]	10.205.119.1	SRX650	10.483.5	New	In Sync	up	View
sd-srx240-4[Hub]	10.205.119.8	SRX240B	10.483.5	New	In Sync	up	View
sd-srx100-5	10.205.119.15	SRX100B	10.483.5	New	In Sync	up	View
10.205.119.11	10.205.119.11	SRX100H	10.483.5	New	In Sync	up	View
10.204.77.19	10.204.77.19	SSG550	6.3.0r1.0	New	In Sync	up	View
10.205.93.5	10.205.93.5	NSISG1000	6.3.0r1.0	New	In Sync	up	View

Impacted Services to be re-provisioned		
Service Name	Service Type	Details
Corporate-Branch	Security Policy	View

☐ Schedule at a later time

[Provision](#) [Cancel](#)

Related Documentation

- IPsec VPNs Overview on page 123
- Creating IPsec VPNs on page 123
- Managing IPsec VPNs on page 133
- Decommissioning IPsec VPNs on page 135

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.

You can either right-click or use the Actions Drawer to manage an IPsec VPN. For more information about using the Actions Drawer, see [Inventory Pages Overview](#)

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

1. Modifying an IPsec VPN on page 134
2. Deleting an IPsec VPN on page 134

Modifying an IPsec VPN

To modify an IPsec VPN you have created:

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 redirects 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. In the **Description** field, enter a new description.
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**.

Deleting an IPsec VPN

To delete an IPsec VPN you have created:

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**.

Related Documentation

- [IPSec VPNs Overview on page 123](#)
- [Creating IPSec VPNs on page 123](#)
- [Deploying IPSec VPNs on page 127](#)

- Decommissioning IPsec VPNs on page 135

Decommissioning IPsec VPNs

To decommission an IPsec VPN you have created:

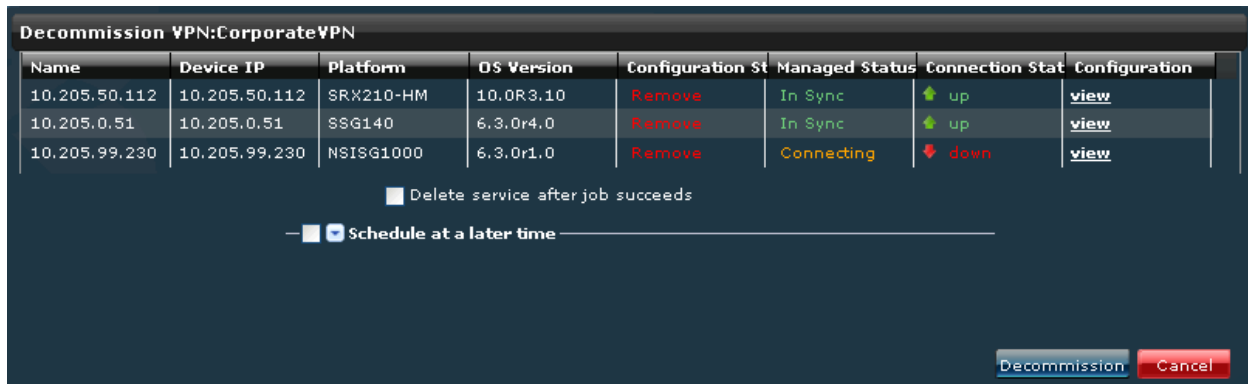
1. From the **Security Design** task ribbon, select **Security Whiteboard** > **IPsec VPN**.

The **Manage VPNs** inventory panel is displayed.

2. Right-click the VPN you want to decommission and select **Decommission VPN** from the contextual menu.

The **Decommission VPN** window displays the devices on which this VPN is provisioned, as shown in Figure 80 on page 135.

Figure 80: Decommission VPN Window



3. To automatically delete the VPN from Junos Space after the VPN is decommissioned, select the **Delete service after job succeeds** check box.
4. To schedule the decommissioning to a later time and date, select the check box next to the **Schedule at a later time** field.
5. Click **Next**.
6. Select appropriate values from the **Date and Time** field.
7. Click **Decommission**.



NOTE: If a provision job on a VPN partially succeeds (that is, the provision job does not push the configuration details to all devices in the VPN), the VPN is placed in the Partially Provisioned state. You can provision or decommission the VPN using the appropriate workflow.



NOTE: If you try to delete a VPN that is in the Provisioned state, a popup window confirming whether you want to decommission the VPN is displayed. You can click **Yes** in this window to decommission the VPN before deleting it, or click **No** to delete the VPN without decommissioning it.

**Related
Documentation**

- [IPSec VPNs Overview on page 123](#)
- [Creating IPSec VPNs on page 123](#)
- [Managing IPSec VPNs on page 133](#)
- [Deploying IPSec VPNs on page 127](#)

PART 5

Index

- Index on page 139

Index

A

address and address groups overview.....	39
addresses	
creating.....	40
deleting.....	44
modifying.....	42
searching.....	44
viewing the details.....	42
application and application groups overview.....	19
application groups	
creating.....	25
deleting.....	29
modifying.....	28
searching.....	29
viewing the details.....	28
applications	
creating.....	20
deleting.....	24
modifying.....	24
searching.....	25
viewing the details.....	24

C

conventions	
notice icons.....	xvii
customer support.....	xviii
contacting JTAC.....	xviii

D

dashboard	
overview.....	5, 7
documentation	
comments on.....	xviii

I

IPsec VPNs	
creating.....	123
decommissioning.....	135
deleting.....	134

deploying.....	127
overview.....	123

M

manuals	
comments on.....	xviii

N

NAT	
NAT policy	
creating.....	87
decommissioning.....	97
managin.....	98
provisioning.....	95
NAT pool	
managing.....	100
overview.....	85
notice icons.....	xvii

O

Object Builder overview.....	17
------------------------------	----

S

Security Design Overview.....	3
security domains	
creating.....	32
deleting.....	36
modifying.....	35
overview.....	31
searching.....	36
viewing the details.....	35
security policies	
creating.....	68
deleting.....	81
deploying.....	74
modifying.....	81
overview.....	66
searching.....	81
viewing the details.....	80
security policy	
decommissioning.....	83

Security Policy Designer.....	68
security policy profiles	
copying.....	65
creating.....	61
deleting.....	66
modifying.....	65
overview.....	59
searching.....	66
viewing the details.....	64
security topology	
adding addresses and security domains using CSV import.....	56
associating addresses with security devices.....	53
connecting security devices.....	52
creating.....	49
creating device groups.....	54
creating group links on device groups.....	56
deleting.....	50
drag and drop security devices.....	51
editing.....	50
overview.....	47
saving.....	50
searching for objects in topology.....	55
Security Whiteboard Overview.....	45
support, technical See technical support	

T

technical support	
contacting JTAC.....	xviii

V

VPN profiles	
copying.....	122
creating.....	112
deleting.....	121
modifying.....	120
overview.....	112
searching.....	122
viewing the details.....	119
VPN proposals	
copying.....	111
creating.....	104
deleting.....	110
modifying.....	109
overview.....	103
searching.....	111
viewing the details.....	108