



Junos[®] OS

Feature Support Reference for SRX Series and J Series Devices

Release
11.2



Published: 2011-05-11

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

Junos OS Feature Support Reference for SRX Series and J Series Devices

Release 11.2

Copyright © 2011, Juniper Networks, Inc.

All rights reserved.

Revision History

May 2011—R1 Junos OS 11.2

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 year 2038. However, the NTP application is known to have some difficulty in the year 2036.

SOFTWARE LICENSE

The terms and conditions for using this software are described in the software license contained in the acknowledgment to your purchase order or, to the extent applicable, to any reseller agreement or end-user purchase agreement executed between you and Juniper Networks. By using this software, you indicate that you understand and agree to be bound by those terms and conditions. Generally speaking, the software license restricts the manner in which you are permitted to use the software and may contain prohibitions against certain uses. The software license may state conditions under which the license is automatically terminated. You should consult the license for further details. For complete product documentation, please see the Juniper Networks website at www.juniper.net/techpubs.

END USER LICENSE AGREEMENT

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

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

2. **The Software.** In this Agreement, “Software” means the program modules and features of the Juniper or Juniper-supplied software, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller, or which was embedded by Juniper in equipment which Customer purchased from Juniper or an authorized Juniper reseller. “Software” also includes updates, upgrades and new releases of such software. “Embedded Software” means Software which Juniper has embedded in or loaded onto the Juniper equipment and any updates, upgrades, additions or replacements which are subsequently embedded in or loaded onto the equipment.

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

a. Customer shall use Embedded Software solely as embedded in, and for execution on, Juniper equipment originally purchased by Customer from Juniper or an authorized Juniper reseller.

b. Customer shall use the Software on a single hardware chassis having a single processing unit, or as many chassis or processing units for which Customer has paid the applicable license fees; provided, however, with respect to the Steel-Belted Radius or Odyssey Access Client software only, Customer shall use such Software on a single computer containing a single physical random access memory space and containing any number of processors. Use of the Steel-Belted Radius or IMS AAA software on multiple computers or virtual machines (e.g., Solaris zones) requires multiple licenses, regardless of whether such computers or virtualizations are physically contained on a single chassis.

c. Product purchase documents, paper or electronic user documentation, and/or the particular licenses purchased by Customer may specify limits to Customer’s use of the Software. Such limits may restrict use to a maximum number of seats, registered endpoints, concurrent users, sessions, calls, connections, subscribers, clusters, nodes, realms, devices, links, ports or transactions, or require the purchase of separate licenses to use particular features, functionalities, services, applications, operations, or capabilities, or provide throughput, performance, configuration, bandwidth, interface, processing, temporal, or geographical limits. In addition, such limits may restrict the use of the Software to managing certain kinds of networks or require the Software to be used only in conjunction with other specific Software. Customer’s use of the Software shall be subject to all such limitations and purchase of all applicable licenses.

d. For any trial copy of the Software, Customer’s right to use the Software expires 30 days after download, installation or use of the Software. Customer may operate the Software after the 30-day trial period only if Customer pays for a license to do so. Customer may not extend or create an additional trial period by re-installing the Software after the 30-day trial period.

e. The Global Enterprise Edition of the Steel-Belted Radius software may be used by Customer only to manage access to Customer’s enterprise network. Specifically, service provider customers are expressly prohibited from using the Global Enterprise Edition of the Steel-Belted Radius software to support any commercial network access services.

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

4. **Use Prohibitions.** Notwithstanding the foregoing, the license provided herein does not permit the Customer to, and Customer agrees not to and shall not: (a) modify, unbundle, reverse engineer, or create derivative works based on the Software; (b) make unauthorized copies of the Software (except as necessary for backup purposes); (c) rent, sell, transfer, or grant any rights in and to any copy of the Software, in any form, to any third party; (d) remove any proprietary notices, labels, or marks on or in any copy of the Software or any product in which the Software is embedded; (e) distribute any copy of the Software to any third party, including as may be embedded in Juniper equipment sold in the secondhand market; (f) use any ‘locked’ or key-restricted feature, function, service, application, operation, or capability without first purchasing the applicable license(s) and obtaining a valid key from Juniper, even if such feature, function, service, application, operation, or capability is enabled without a key; (g) distribute any key for the Software provided by Juniper to any third party; (h) use the

Software in any manner that extends or is broader than the uses purchased by Customer from Juniper or an authorized Juniper reseller; (i) use Embedded Software on non-Juniper equipment; (j) use Embedded Software (or make it available for use) on Juniper equipment that the Customer did not originally purchase from Juniper or an authorized Juniper reseller; (k) disclose the results of testing or benchmarking of the Software to any third party without the prior written consent of Juniper; or (l) use the Software in any manner other than as expressly provided herein.

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

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

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

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

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

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

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

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

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

14. **Third Party Software.** Any licensor of Juniper whose software is embedded in the Software and any supplier of Juniper whose products or technology are embedded in (or services are accessed by) the Software shall be a third party beneficiary with respect to this Agreement, and such licensor or vendor shall have the right to enforce this Agreement in its own name as if it were Juniper. In addition, certain third party software may be provided with the Software and is subject to the accompanying license(s), if any, of its respective owner(s). To the extent portions of the Software are distributed under and subject to open source licenses obligating Juniper to make the source code for such portions publicly available (such as the GNU General Public License ("GPL") or the GNU Library General Public License ("LGPL")), Juniper will make such source code portions (including Juniper modifications, as appropriate) available upon request for a period of up to three years from the date of distribution. Such request can be made in writing to Juniper Networks, Inc., 1194 N. Mathilda Ave., Sunnyvale, CA 94089, ATTN: General Counsel. You may obtain a copy of the GPL at <http://www.gnu.org/licenses/gpl.html>, and a copy of the LGPL at <http://www.gnu.org/licenses/lgpl.html>.

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

Table of Contents

	About This Guide	ix
	J Series and SRX Series Documentation and Release Notes	ix
	Supported Routing Platforms	ix
	Document Conventions	x
	Documentation Feedback	xi
	Requesting Technical Support	xii
	Self-Help Online Tools and Resources	xii
	Opening a Case with JTAC	xii
Part 1	Feature Support for SRX Series and J Series Devices	
Chapter 1	Juniper Networks Devices' Feature Support	3
	Feature Support Overview	3
Chapter 2	Feature Support Tables	5
	Address Books and Address Sets	6
	Administrator Authentication	7
	Alarms	8
	Application Identification (Junos OS)	9
	Application Layer Gateways	9
	Attack Detection and Prevention	11
	Authentication with IC Series Devices	12
	Autoinstallation	13
	Chassis Cluster	13
	Chassis Management	15
	Class of Service	16
	Dynamic Host Configuration Protocol	17
	Dynamic VPN	17
	Diagnostics Tools	18
	Ethernet Link Aggregation	19
	File Management	20
	Firewall Authentication	20
	Flow-Based and Packet-Based Processing	21
	General Packet Radio Service	22
	Interfaces	23
	Intrusion Detection and Prevention	27
	IP Security	29
	IPv6 Support	31
	IPv6 IP Security	33
	Junos OS Feature Licenses	34
	Layer 2 Mode	35

Logical Systems	36
Management	38
MPLS	38
Multicast	40
Multicast VPN	41
Network Address Translation	42
Network Operations and Troubleshooting	43
Packet Capture	44
Power over Ethernet	44
Public Key Infrastructure	45
Real-Time Performance Monitoring Probe	46
Remote Device Access	47
Routing	47
Secure Web Access	49
Security Policy	49
Security Zone	51
Session Logging	52
SMTP	52
SNMP	53
Stateless Firewall Filters	53
System Log Files	54
Transparent Mode	55
Unified Threat Management	55
Upgrading and Rebooting	56
USB Modem	57
User Interfaces	57
Voice over Internet Protocol with Avaya	58
Wireless Local Area Network	59

Part 2

Index

Index	63
-----------------	----

About This Guide

This preface provides the following guidelines for using the *Junos OS Feature Support Reference for SRX Series and J Series Devices*:

- J Series and SRX Series Documentation and Release Notes on page ix
- Supported Routing Platforms on page ix
- Document Conventions on page x
- Documentation Feedback on page xi
- Requesting Technical Support on page xii

J Series and SRX Series Documentation and Release Notes

For a list of related J Series documentation, see <http://www.juniper.net/techpubs/software/junos-jseries/index-main.html> .

For a list of related SRX Series documentation, see <http://www.juniper.net/techpubs/hardware/srx-series-main.html> .

If the information in the latest release notes differs from the information in the documentation, follow the *Junos OS 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/> .

Juniper Networks supports a technical book program to publish books by Juniper Networks engineers and subject matter experts with book publishers around the world. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration using the Junos operating system (Junos OS) and Juniper Networks devices. In addition, the Juniper Networks Technical Library, published in conjunction with O'Reilly Media, explores improving network security, reliability, and availability using Junos OS configuration techniques. All the books are for sale at technical bookstores and book outlets around the world. The current list can be viewed at <http://www.juniper.net/books> .

Supported Routing Platforms

This manual describes features supported on J Series Services Routers and SRX Series Services Gateways running Junos OS.

Document Conventions

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

Table 1: Notice Icons

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

Table 2 on page x defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: user@host> configure
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> show chassis alarms No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces important new terms. Identifies book names. Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS System Basics Configuration Guide</i> RFC 1997, <i>BGP Communities Attribute</i>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i>

Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
Text like this	Represents names of configuration statements, commands, files, and directories; interface names; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> To configure a stub area, include the stub statement at the <code>[edit protocols ospf area area-id]</code> hierarchy level. The console port is labeled CONSOLE.
< > (angle brackets)	Enclose optional keywords or variables.	stub <default-metric <i>metric</i> >;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast <i>(string1 string2 string3)</i>
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Enclose a variable for which you can substitute one or more values.	community name members [community-ids]
Indentation and braces ({ })	Identify a level in the configuration hierarchy.	<code>[edit] routing-options { static { route default { nexthop <i>address</i>; retain; } } }</code>
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
J-Web GUI Conventions		
Bold text like this	Represents J-Web graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> In the Logical Interfaces box, select All Interfaces. To cancel the configuration, click Cancel.
> (bold right angle bracket)	Separates levels in a hierarchy of J-Web selections.	In the configuration editor hierarchy, select Protocols>Ospf .

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 postsales technical support, you can access our tools and resources online or open a case with JTAC.

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

Self-Help Online Tools and Resources

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

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- 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, visit us at <http://www.juniper.net/support/requesting-support.html>

PART 1

Feature Support for SRX Series and J Series Devices

- Juniper Networks Devices' Feature Support on page 3
- Feature Support Tables on page 5

CHAPTER 1

Juniper Networks Devices' Feature Support

- Feature Support Overview on page 3

Feature Support Overview

This guide provides feature support information for SRX Series Services Gateways and J Series Services Routers and specifies which hardware devices support those features.

Powered by the Junos operating system (Junos OS), Juniper Networks SRX Series Services Gateways provide robust networking and security services. SRX Series Services Gateways range from lower-end devices designed to secure small distributed enterprise locations to high-end devices designed to secure enterprise infrastructure, data centers, and server farms. The SRX Series Services Gateways include the following devices:

- SRX100
- SRX210
- SRX220
- SRX240
- SRX650
- SRX1400
- SRX3400
- SRX3600
- SRX5600
- SRX5800

Juniper Networks J Series Services Routers running Junos OS provide stable, reliable, and efficient IP routing, WAN and LAN connectivity, and management services for small to medium-sized enterprise networks. These devices also provide network security features, including a stateful firewall with access control policies and screens to protect against attacks and intrusions, and IP Security virtual private networks (IPsec VPNs). The J Series Services Routers include the following devices:

- J2320
- J2350
- J4350
- J6350

**Related
Documentation**

- [*Junos OS Initial Configuration Guide for Security Devices*](#)
- [*Junos OS Monitoring and Troubleshooting Guide for Security Devices*](#)
- [*Junos OS Interfaces and Routing Configuration Guide*](#)
- [*Junos OS Security Configuration Guide*](#)

CHAPTER 2

Feature Support Tables

- Address Books and Address Sets on page 6
- Administrator Authentication on page 7
- Alarms on page 8
- Application Identification (Junos OS) on page 9
- Application Layer Gateways on page 9
- Attack Detection and Prevention on page 11
- Authentication with IC Series Devices on page 12
- Autoinstallation on page 13
- Chassis Cluster on page 13
- Chassis Management on page 15
- Class of Service on page 16
- Dynamic Host Configuration Protocol on page 17
- Dynamic VPN on page 17
- Diagnostics Tools on page 18
- Ethernet Link Aggregation on page 19
- File Management on page 20
- Firewall Authentication on page 20
- Flow-Based and Packet-Based Processing on page 21
- General Packet Radio Service on page 22
- Interfaces on page 23
- Intrusion Detection and Prevention on page 27
- IP Security on page 29
- IPv6 Support on page 31
- IPv6 IP Security on page 33
- Junos OS Feature Licenses on page 34
- Layer 2 Mode on page 35
- Logical Systems on page 36
- Management on page 38

- MPLS on page 38
- Multicast on page 40
- Multicast VPN on page 41
- Network Address Translation on page 42
- Network Operations and Troubleshooting on page 43
- Packet Capture on page 44
- Power over Ethernet on page 44
- Public Key Infrastructure on page 45
- Real-Time Performance Monitoring Probe on page 46
- Remote Device Access on page 47
- Routing on page 47
- Secure Web Access on page 49
- Security Policy on page 49
- Security Zone on page 51
- Session Logging on page 52
- SMTP on page 52
- SNMP on page 53
- Stateless Firewall Filters on page 53
- System Log Files on page 54
- Transparent Mode on page 55
- Unified Threat Management on page 55
- Upgrading and Rebooting on page 56
- USB Modem on page 57
- User Interfaces on page 57
- Voice over Internet Protocol with Avaya on page 58
- Wireless Local Area Network on page 59

Address Books and Address Sets

Junos OS supports address books and address sets. An address book is a collection of addresses and address sets that are available in one security zone.

An address in an address book could be a name for an IP address, a network prefix, a DNS domain, or a range of IP addresses. Address sets are collections of addresses within an address book. They allow you to effectively manage addresses when configuring your network. Instead of managing large numbers of individual address entries, you can more easily manage a smaller number of address sets because any change made to an address set automatically apply to all the addresses in the set.

Junos OS also supports a global address book, which is created on each system by default. It contains predefined addresses and is not attached to any zone.

Table 3 on page 7 lists the address book features supported on SRX Series and J Series devices.

Table 3: Address Books and Address Sets Support

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Address books	Yes	Yes	Yes	Yes
Address sets	Yes	Yes	Yes	Yes
Global address objects or sets	No	No	Yes	No
Nested address groups	No	No	Yes	No

Related Documentation • [Junos OS Security Configuration Guide](#)

Administrator Authentication

Junos OS supports three methods of administrator authentication:

- Local password authentication
- RADIUS
- TACACS+

With local password authentication, you configure a password for each user who is allowed to log in to the device.

RADIUS and TACACS+ are authentication methods for validating users who attempt to access the device using Telnet, SSH or other administrative means. Both are distributed client/server systems—the RADIUS and TACACS+ clients run on the device, and the server runs on a remote network system.

Table 4 on page 7 lists the administrator authentication features that are supported on SRX Series and J Series devices.

Table 4: Administrator Authentication Support

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800
Local authentication	Yes	Yes	Yes

Table 4: Administrator Authentication Support (*continued*)

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800
RADIUS	Yes	Yes	Yes
TACACS+	Yes	Yes	Yes

Related Documentation

- [Junos OS Initial Configuration Guide for Security Devices](#)

Alarms

Junos OS supports three types of alarms:

- Chassis alarms indicate a failure on the device or one of its components. Chassis alarms are preset and cannot be modified.
- Interface alarms indicate a problem in the state of the physical links on fixed or installed PIMs. To enable interface alarms, you must configure them.
- System alarms indicate a missing rescue configuration or software license, where valid. System alarms are preset and cannot be modified, although you can configure them to appear automatically in the J-Web or CLI display.

Table 5 on page 8 lists the alarm features that are supported on SRX Series and J Series devices.

Table 5: Alarm Support

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Chassis alarms	Yes	Yes	Yes	Yes
Interface alarms	Yes	Yes	Yes	Yes
System alarms	Yes	Yes	Yes	Yes

Related Documentation

- [Junos OS Monitoring and Troubleshooting Guide for Security Devices](#)

Application Identification (Junos OS)

Juniper Networks provides predefined application signatures that detect TCP and UDP applications running on nonstandard ports. Identifying these applications allows Intrusion Detection and Prevention (IDP) to apply appropriate attack objects to applications running on nonstandard ports and provides data for application tracking (AppTrack), Application Firewall (AppFW), and Application DDoS.



NOTE: The information in Table 6 on page 9 refers to the Junos OS application identification module located in the services hierarchy.

Table 6: Application Identification

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Application DDoS	No	No	Yes	No
Application Firewall (AppFW)	Yes	Yes	Yes	No
Application Tracking (AppTrack)	Yes	Yes	Yes	No
Encrypted application heuristics	No	No	Yes	No
IDP	Yes	Yes	Yes	Yes
Custom application signatures	No	No	Yes (CLI only)	No

Related Documentation • [Intrusion Detection and Prevention on page 27](#)

Application Layer Gateways

An Application Layer Gateway (ALG) is a software component that is designed to manage specific protocols such as Session Initiation Protocol (SIP) or File Transfer Protocol (FTP) on SRX Series and J Series devices running Junos OS. The ALG intercepts and analyzes the specified traffic, allocates resources, and defines dynamic policies to permit the traffic to pass securely through the Juniper Networks device. Also, ALGs modify the embedded IP addresses as required.

Table 7 on page 10 lists the ALG features that are supported on SRX Series and J Series devices.

Table 7: ALG Support

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
DNS ALG	Yes	Yes	Yes	Yes
DNS doctoring support	Yes	Yes	Yes	Yes
DNS, FTP, RTSP, and TFTP ALGs (Layer 2) with chassis clustering	Yes	Yes	Yes	No
DSCP marking for SIP, H.323, MGCP, and SCCP ALGs	Yes	Yes	Yes	Yes
FTP	Yes	Yes	Yes	Yes
H.323	Yes	Yes	No	Yes
Avaya H.323	Yes	Yes	No	Yes
MGCP	Yes	Yes	No	Yes
PPTP	Yes	Yes	Yes	Yes
RSH	Yes	Yes	Yes	Yes
RTSP	Yes	Yes	Yes	Yes
SCCP	Yes	Yes	No	Yes
SIP	Yes	Yes	Yes	Yes
SIP ALG–NEC	Yes	Yes	Yes	Yes
SQL	Yes	Yes	Yes	Yes
MS RPC	Yes	Yes	Yes	Yes
SUN RPC	Yes	Yes	Yes	Yes
TALK	Yes	Yes	Yes	Yes
TFTP	Yes	Yes	Yes	Yes

Related Documentation • [Junos OS Security Configuration Guide](#)

Attack Detection and Prevention

Attack detection and prevention, also known as a *stateful firewall*, detects and prevents attacks in network traffic. An exploit can be either an information-gathering probe or an attack to compromise, disable, or harm a network or network resource.

Juniper Networks provides various detection methods and defense mechanisms at the zone and policy levels to combat exploits at all stages of their execution, including:

- Screen options at the zone level
- Firewall policies at the inter-, intra-, and super-zone policy levels (super-zone here means in global policies, where no security zones are referenced)

Table 8 on page 11 lists attack detection and prevention features (screens) that are supported on SRX Series and J Series devices.

Table 8: Attack Detection and Prevention Support (Screens)

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Bad IP option	Yes	Yes	Yes	Yes
Block fragment traffic	Yes	Yes	Yes	Yes
FIN flag without ACK flag set protection	Yes	Yes	Yes	Yes
ICMP flood protection	Yes	Yes	Yes	Yes
ICMP fragment protection	Yes	Yes	Yes	Yes
IP address spoof	Yes	Yes	Yes	Yes
IP address sweep	Yes	Yes	Yes	Yes
IP record route option	Yes	Yes	Yes	Yes
IP security option	Yes	Yes	Yes	Yes
IP stream option	Yes	Yes	Yes	Yes
IP strict source route option	Yes	Yes	Yes	Yes
IP timestamp option	Yes	Yes	Yes	Yes
Land attack protection	Yes	Yes	Yes	Yes
Large size ICMP packet protection	Yes	Yes	Yes	Yes

Table 8: Attack Detection and Prevention Support (Screens) (*continued*)

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Loose source route option	Yes	Yes	Yes	Yes
Ping of death attack protection	Yes	Yes	Yes	Yes
Port scan	Yes	Yes	Yes	Yes
Source IP-based session limit	Yes	Yes	Yes	Yes
SYN-ACK-ACK proxy protection	Yes	Yes	Yes	Yes
SYN and FIN flags set protection	Yes	Yes	Yes	Yes
SYN flood protection	Yes	Yes	Yes	Yes
SYN fragment protection	Yes	Yes	Yes	Yes
TCP address sweep	Yes	Yes	Yes	Yes
TCP packet without flag set protection	Yes	Yes	Yes	Yes
Teardrop attack protection	Yes	Yes	Yes	Yes
UDP address sweep	Yes	Yes	Yes	Yes
UDP flood protection	Yes	Yes	Yes	Yes
Unknown protocol protection	Yes	Yes	Yes	Yes
WinNuke attack protection	Yes	Yes	Yes	Yes

- Related Documentation**
- [Junos OS Security Configuration Guide](#)
 - Intrusion Detection and Prevention on page 27

Authentication with IC Series Devices

A Unified Access Control (UAC) deployment uses IC Series devices, UAC Enforcers, and UAC Agents to secure a network and ensure that only qualified end users can access protected resources. An SRX Series or J Series device can act as a UAC Enforcer in a UAC network. Specifically, it acts as a Layer 3 enforcement point, controlling access by using IP-based policies pushed down from the IC Series devices. When deployed in a UAC network, an SRX Series or J Series device is called a *Junos OS Enforcer*.

Table 9 on page 13 lists support for authentication with IC Series devices on SRX Series and J Series devices.

Table 9: Supported Features for Authentication with IC Series Devices

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Captive portal	Yes	Yes	Yes	Yes
Junos OS Enforcers in UAC deployments	Yes	Yes	Yes	Yes

Related Documentation • [Junos OS Security Configuration Guide](#)

Autoinstallation

Autoinstallation provides automatic configuration for a new device that you connect to the network and turn on, or for a device configured for autoinstallation. The autoinstallation process begins any time a device is powered on and cannot locate a valid configuration file in the CompactFlash card. Typically, a configuration file is unavailable when a device is powered on for the first time, or if the configuration file is deleted from the CompactFlash card. The autoinstallation feature enables you to deploy multiple devices from a central location in the network.

Table 10 on page 13 lists the autoinstallation support on SRX Series and J Series devices.

Table 10: Autoinstallation Support

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Autoinstallation	Yes	Yes	No	Yes

Related Documentation • [Junos OS Initial Configuration Guide for Security Devices](#)

Chassis Cluster

Chassis clustering provides network node redundancy by grouping a pair of the same kind of supported SRX Series devices or J Series devices into a cluster. The devices must be running Junos OS.

Table 11 on page 14 lists chassis cluster features that are supported on SRX Series and J Series devices.

Table 11: Chassis Cluster Support

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Active/active chassis cluster (that is, cross-box data forwarding over the fabric interface)	Yes	Yes	Yes	Yes
ALGs	Yes	Yes	Yes	Yes
Chassis cluster formation	Yes	Yes	Yes	Yes
Control plane failover	Yes	Yes	Yes	Yes
Dampening time between back-to-back redundancy group failovers	Yes	Yes	Yes	Yes
Data plane failover	Yes	Yes	Yes	Yes
Dual control links	No	No	Yes	No
Dual fabric links	Yes	Yes	Yes	Yes
Junos OS flow-based routing functionality	Yes	Yes	Yes	Yes
Layer 2 Ethernet switching capability	SRX240 only	Yes	No	No
Layer 2 LAG	SRX240 only	Yes	Yes	No
Layer 3 LAG	Yes	Yes	Yes	No
LACP support for layer 2	Yes	Yes	No	No
LACP support for layer 3	Yes	Yes	Yes	No
Low-impact cluster upgrade (ISSU light)	No	No	Yes	No
Multicast routing	Yes	Yes	Yes	Yes

Table 11: Chassis Cluster Support (*continued*)

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Redundant Ethernet interfaces	Yes	Yes	Yes	Yes
Redundant Ethernet interface LAGs	Yes	No	Yes	No
Redundant Ethernet or aggregate Ethernet interface monitoring	Yes	Yes	Yes	Yes
Redundancy group 0 (backup for Routing Engine)	Yes	Yes	Yes	Yes
Redundancy groups 1 through 128	Yes	Yes	Yes	Yes
Upstream device IP address monitoring	No	No	Yes	No
Upstream device IP address monitoring on a backup interface	No	No	Yes	No

Related Documentation • [Junos OS Security Configuration Guide](#)

Chassis Management

The chassis properties include the status of hardware components on the device.

Table 12 on page 15 lists the chassis management support on SRX Series and J Series devices.

Table 12: Chassis Management Support

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Chassis management	Yes	Yes	Yes	Yes

- Related Documentation**
- [Junos OS Initial Configuration Guide for Security Devices](#)
 - [Junos OS Monitoring and Troubleshooting Guide for Security Devices](#)

Class of Service

When a network experiences congestion and delay, some packets must be dropped. Junos OS class of service (CoS) allows you to divide traffic into classes and offer various levels of throughput and packet loss when congestion occurs. This allows packet loss to happen according to the rules you configure.

Table 13 on page 16 lists the CoS features that are supported on SRX Series and J Series devices.

Table 13: CoS Support

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Classifiers	Yes	Yes	Yes	Yes
Code-point aliases	Yes	Yes	Yes	Yes
Egress interface shaping	Yes	Yes	No	Yes
Forwarding classes	Yes	Yes	Yes	Yes
Ingress interface policer	Yes	Yes	Yes	Yes
Schedulers	Yes	Yes	Yes	Yes
Simple filters	No	No	Yes	No
Transmission queues	Yes	Yes	Yes	Yes
Tunnels	Yes	Yes	Yes	Yes
			NOTE: GRE and IP-IP tunnels only.	
Virtual channels	Yes	Yes	No	Yes

- Related Documentation**
- [Junos OS Class of Service Configuration Guide for Security Devices](#)

Dynamic Host Configuration Protocol

Dynamic Host Configuration Protocol (DHCP) is based on BOOTP, a bootstrap protocol that allows a client to discover its own IP address, the IP address of a server host, and the name of a bootstrap file. DHCP servers can handle requests from BOOTP clients, but provide additional capabilities beyond BOOTP, such as the automatic allocation of reusable IP addresses and additional configuration options.

DHCP provides two primary functions:

- Allocate temporary or permanent IP addresses to clients.
- Store, manage, and provide client configuration parameters.

Table 14 on page 17 lists the DHCP features that are supported on SRX Series and J Series devices.

Table 14: DHCP Support

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
DHCP client	Yes	Yes	Yes	Yes
DHCPv6	No	No	Yes	No
DHCP relay agent	Yes	Yes	Yes	Yes
DHCP server	Yes	Yes	Yes	Yes
DHCP server address pools	Yes	Yes	Yes	Yes
DHCP server static mapping	Yes	Yes	Yes	Yes

Related Documentation • [Junos OS Initial Configuration Guide for Security Devices](#)

Dynamic VPN

Virtual private network (VPN) tunnels enable users to securely access assets such as e-mail servers and application servers that reside behind a firewall. End-to-site VPN tunnels are particularly helpful to remote users such as telecommuters because a single tunnel enables access to all of the resources on a network—the users do not need to configure individual access settings for each application and server.

The dynamic VPN feature further simplifies remote access by enabling users to establish Internet Protocol Security (IPsec) VPN tunnels without having to manually configure VPN settings on their PCs or laptops. Instead, authenticated users can simply download

the Access Manager Web client to their computers. This Layer 3 remote access client uses client-side configuration settings that it receives from the server to create and manage a secure end-to-site VPN tunnel to the server.

Table 15 on page 18 lists the dynamic VPN features that are supported on SRX Series and J Series devices.

Table 15: Dynamic VPN Support

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Package dynamic VPN client	SRX100, SRX210, and SRX240 only	Yes	No	No

Related Documentation

- [Junos OS Security Configuration Guide](#)

Diagnostics Tools

SRX Series and J Series devices support a suite of J-Web tools and CLI operational mode commands for evaluating system health and performance. Diagnostics tools and commands test the connectivity and reachability of hosts in the network.

Table 16 on page 18 lists the diagnostics tools features that are supported on SRX Series and J Series devices.

Table 16: Diagnostics Tools Support

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
CLI terminal	Yes	Yes	Yes	Yes
J-Flow versions 5 and version 8	Yes	Yes	Yes	Yes
J-Flow version 9	Yes	Yes	No	Yes
Ping host	Yes	Yes	Yes	Yes
Ping MPLS	Yes	Yes	No	Yes
Traceroute	Yes	Yes	Yes	Yes

Related Documentation

- [Junos OS Monitoring and Troubleshooting Guide for Security Devices](#)

Ethernet Link Aggregation

Link aggregation groups (LAGs) based on IEEE 802.3ad make it possible to aggregate physical interface links on a device. LAGs provide increased interface bandwidth and link availability by linking physical ports and load-balancing traffic crossing the combined interface.

Link aggregation extends to chassis cluster configurations, allowing a redundant Ethernet interface to add multiple child interfaces from both nodes and thereby create a redundant Ethernet interface link aggregation group. For a list of chassis cluster features that are supported on SRX Series and J Series devices, see “Chassis Cluster” on page 13.

The Link Aggregation Control Protocol (LACP), a subcomponent of IEEE 802.3ad, provides additional functionality for LAGs. LACP is supported in standalone deployments, where aggregated Ethernet interfaces are supported, and in chassis cluster deployments, where aggregated Ethernet interfaces and redundant Ethernet interfaces are supported simultaneously.

Table 17 on page 19 lists the Ethernet link aggregation features that are supported on SRX Series and J Series devices.

Table 17: Ethernet Link Aggregation Support

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Routing mode				
LACP in chassis cluster mode	No	No	Yes	No
LACP in standalone mode	Yes	No	Yes	Yes
Link aggregation in chassis cluster mode	No	Yes	Yes	No
Link aggregation in standalone mode	Yes	No	Yes	Yes
Layer 3 LAG on routed ports	Yes	Yes	Yes	Yes
Transparent mode	No	No	Yes	No
Switching mode				
LACP in chassis cluster mode	No	No	–	No
LACP in standalone mode	Yes	Yes	–	Yes
Link aggregation in chassis cluster mode	No	No	–	No
Link aggregation in standalone mode	Yes	Yes	–	Yes

- Related Documentation**
- [Junos OS Initial Configuration Guide for Security Devices](#)
 - [Junos OS Interfaces Configuration Guide for Security Devices](#)
 - [Junos OS Layer 2 Bridging and Switching Configuration Guide for Security Devices](#)

File Management

You can use the J-Web interface to perform routine file management operations such as archiving log files and deleting unused log files, cleaning up temporary files and crash files, and downloading log files from the routing platform to your computer. You can also encrypt the configuration files with the CLI configuration editor to prevent unauthorized users from viewing sensitive configuration information.

Table 18 on page 20 lists the file management features that are supported on SRX Series and J Series devices.

Table 18: File Management Support

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Clean up unnecessary files	Yes	Yes	Yes	Yes
Delete backup software image	Yes	Yes	Yes	Yes
Delete individual files	Yes	Yes	Yes	Yes
Download system files	Yes	Yes	Yes	Yes
Encrypt/decrypt configuration files	Yes	Yes	Yes	Yes
Manage account files	Yes	Yes	No	Yes

- Related Documentation**
- [Junos OS Monitoring and Troubleshooting Guide for Security Devices](#)

Firewall Authentication

Junos OS supports the following two types of firewall user authentication:

- **Pass-through authentication**—A host or a user from one zone tries to access resources on another zone. You must use an FTP, Telnet, or HTTP client to access the IP address of the protected resource and to get authenticated by the firewall. The device uses FTP, Telnet, or HTTP to collect username and password information. Subsequent traffic from the user or host is allowed or denied based on the result of this authentication.

- Web authentication—Users try to connect, using HTTP, to an IP address on the device that is enabled for Web authentication; in this scenario, you do not use HTTP to get to the IP address of the protected resource. You are prompted for the username and password that are verified by the device. Subsequent traffic from the user or host to the protected resource is allowed or denied based on the result of this authentication.

Table 19 on page 21 lists firewall authentication features that are supported on SRX Series and J Series devices.

Table 19: Firewall Authentication Support

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Firewall authentication on Layer 2 transparent authentication	Yes	Yes	Yes	No
LDAP authentication server	Yes	Yes	Yes	Yes
Local authentication server	Yes	Yes	Yes	Yes
Pass-through authentication	Yes	Yes	Yes	Yes
RADIUS authentication server	Yes	Yes	Yes	Yes
SecurID authentication server	Yes	Yes	Yes	Yes
Web authentication	Yes	Yes	Yes	Yes

Related Documentation • [Junos OS Security Configuration Guide](#)

Flow-Based and Packet-Based Processing

A packet undergoes flow-based processing after any packet-based filters and policers have been applied to it. A *flow* is a stream of related packets that meet the same matching criteria and share the same characteristics. Junos OS treats packets belonging to the same flow in the same manner.

A packet undergoes packet-based processing when it is dequeued from its input (ingress) interface and before it is enqueued on its output (egress) interface. Packet-based processing applies stateless firewall filters and class-of-service (CoS) features to discrete packets. You can apply a firewall filter to an ingress or egress interface, or to both.

Table 20 on page 22 lists flow-based and packet-based features that are supported on SRX Series and J Series devices.

Table 20: Flow-Based and Packet-Based Processing Support

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Alarms and auditing	Yes	Yes	No	No
End-to-end packet debugging	No	No	Yes	No
Flow-based processing	Yes	Yes	Yes	Yes
Network processor bundling	No	No	SRX5600 and SRX5800 only	No
Packet-based processing	Yes	Yes	No	Yes
Selective stateless packet-based services	Yes	Yes	No	Yes

Related Documentation • [Junos OS Security Configuration Guide](#)

General Packet Radio Service

General Packet Radio Service (GPRS) networks connect to several external networks, including those of roaming partners, corporate customers, GPRS Roaming Exchange (GRX) providers, and the public Internet. GPRS network operators face the challenge of protecting their network while providing and controlling access to and from these external networks. Juniper Networks provides solutions to many of the security problems plaguing GPRS network operators.

In the GPRS architecture, the fundamental cause of security threats to an operator's network is the inherent lack of security in GPRS tunneling protocol (GTP). GTP is the protocol used between GPRS support nodes (GSNs). Communication between different GPRS networks is not secure, because GTP does not provide any authentication, data integrity, or confidentiality protection. Implementing Internet Protocol security (IPsec) for connections between roaming partners, setting traffic rate limits, and using stateful inspection can eliminate a majority of the GTP's security risks. Juniper Networks security devices mitigate a wide variety of attacks on the Gp, Gn, and Gi interfaces. The GTP firewall features in Junos OS address key security issues in mobile operators' networks.

Table 21 on page 23 lists GPRS features that are supported on SRX Series and J Series devices.

Table 21: GPRS Support

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
GPRS	No	No	Yes	No

Related Documentation • [Junos OS Security Configuration Guide](#)

Interfaces

All Juniper Networks devices use network interfaces to connect to other devices. A connection takes place along media-specific physical wires through a port on a Physical Interface Module (PIMs, uPIMs, ePIMs) installed in the J Series Services Router or an I/O Card (IOC) in the SRX Series Services Gateway. SRX100, SRX210, SRX220, and SRX240 devices support Mini-PIMs, whereas SRX650 devices support XPIMs and GPIMs. Each device interface has a unique name that follows a naming convention.

You must configure each network interface before it can operate on the device. Configuring an interface can define both the physical properties of the link and the logical properties of a logical interface on the link.

Table 22 on page 23 lists the physical and virtual interfaces features that are supported on SRX Series and J Series devices.

Table 22: Physical and Virtual Interface Support

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
1-Port Gigabit Ethernet SFP Mini-PIM interface	Yes	No	No	No
10-Gigabit Ethernet interface	No	Yes	Yes	No
10-Gigabit Ethernet Interface SFP+ slots	No	Yes	SRX1400 only	No
10-Gigabit Ethernet interface XFP slots	No	No	Yes	No
3G wireless modem ExpressCard slot interface	SRX210 only	No	No	No

Table 22: Physical and Virtual Interface Support (*continued*)

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
3G wireless modem interface using the CX-111 external wireless bridge	Yes	Yes	No	Yes
ADSL interface	SRX210, SRX220, and SRX240 only	No	No	Yes
Channelized E1/T1 interface	No	No	No	Yes
Channelized ISDN PRI interface	No	No	No	Yes
Discard interface	Yes	Yes	Yes	Yes
DOCSIS Mini-PIM interface	SRX210, SRX220, and SRX240 only	No	No	No
DS3/E3 interface	No	Yes	No	Yes
Ethernet interface	Yes	Yes	Yes	Yes
Fast Ethernet interface	Yes	Yes	No	Yes
Fractional T1/E1 interface	SRX210, SRX220, and SRX240 only	Yes	No	Yes
Frame Relay interface	SRX210, SRX220, and SRX240 only	Yes	No	Yes
Gigabit Ethernet, Copper (10-Mbps, 100-Mbps, or 1000-Mbps port)	SRX210, SRX220, and SRX240 only	Yes	Yes	Yes
Gigabit Ethernet interface	Yes	Yes	Yes	Yes
ISDN BRI interface	No	No	No	Yes
Serial interface	SRX210, SRX220, and SRX240 only	No	No	Yes

Table 22: Physical and Virtual Interface Support (*continued*)

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Symmetric high-speed digital subscriber line (G.SHDSL) interface	SRX210, SRX220, and SRX240 only	No	No	Yes
T3 interface	No	No	No	Yes
USB modem physical interface	Yes	No	No	Yes
VDSL interface	SRX210, SRX220, and SRX240	No	No	No

Table 23 on page 25 lists the services features that are supported on SRX Series and J Series devices.

Table 23: Services Support

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Aggregated Ethernet interface	Yes	Yes	Yes	Yes
GRE interface	Yes	Yes	Yes	Yes
HDLC interface	SRX210, SRX220, and SRX240 only.	Yes	No	Yes
IEEE 802.1X dynamic VLAN assignment	SRX210, SRX220, and SRX240 only.	Yes	No	No
IEEE 802.1X MAC bypass	Yes	Yes	No	Yes
IEEE 802.1X port-based authentication control with multi-suplicant support	Yes	Yes	No	Yes
Interleaving using MLFR	Yes	Yes	No	Yes

Table 23: Services Support (continued)

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Internally configured interface used by the system as a control path between the WXC Integrated Services Module and the Routing Engine	No	No	No	Yes
Internally generated GRE interface (gr-0/0/0)	Yes	Yes	Yes	Yes
Internally generated IP-over-IP interface (ip-0/0/0)	Yes	Yes	Yes	Yes
Internally generated link services interface	Yes	Yes	No	Yes
Internally generated Protocol Independent Multicast de-encapsulation interface	Yes	No	Yes	Yes
Internally generated Protocol Independent Multicast encapsulation interface	Yes	Yes	Yes	Yes
IP-over-IP encapsulation interface	Yes	Yes	Yes	Yes
Link fragmentation and interleaving interface	Yes	Yes	No	No
Link services interface	Yes	Yes	No	Yes
Loopback interface	Yes	Yes	Yes	Yes
Management interface	Yes	Yes	Yes	Yes
Passive monitoring interface	Yes	Yes	No	Yes

Table 23: Services Support (*continued*)

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
PPP interface	Yes	Yes	No	Yes
PPPoE-based radio-to-router protocol	Yes	Yes	Yes	Yes
PPPoE interface	SRX210, SRX220, and SRX240 only	Yes	No	No
Promiscuous mode on interfaces	No	No	Yes	No
Protocol Independent Multicast de-encapsulation interface	Yes	No	No	Yes
Protocol Independent Multicast encapsulation interface	Yes	No	No	Yes
Redundant Ethernet interface	Yes	Yes	Yes	Yes
Secure tunnel interface	Yes	Yes	Yes	Yes

Related Documentation • [Junos OS Interfaces Configuration Guide for Security Devices](#)

Intrusion Detection and Prevention

The Junos OS Intrusion Detection and Prevention (IDP) policy enables you to selectively enforce various attack detection and prevention techniques on network traffic passing through an IDP-enabled device. It allows you to define policy rules to match traffic based on a zone, network, and application, and then take active or passive preventive actions on that traffic.

Table 24 on page 28 lists IDP features that are supported on SRX Series and J Series devices.

Table 24: IDP Support

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Access control on IDP audit logs	Yes	Yes	No	No
Alarms and auditing	Yes	Yes	Yes	No
Application identification See the Junos OS Application Identification "Application Identification (Junos OS)" on page 9 for the Junos OS version of application identification.	Yes	Yes	Yes	Yes
Application-level DDoS rule base	No	No	Yes	No
Cryptographic key handling	No	No	Yes	No
DSCP marking	Yes	Yes	Yes	Yes
IDP and UAC coordinated threat control	Yes	Yes	Yes	No
IDP class-of-service action	No	No	Yes	No
IDP in an active/active chassis cluster	SRX100, SRX210, and SRX240 only	Yes	Yes	No
IDP inline tap mode	No	No	Yes	No
IDP logging	Yes	Yes	Yes	Yes
IDP monitoring and debugging	Yes	Yes	Yes	Yes
IDP policy	Yes	Yes	Yes	Yes
IDP security packet capture	No	No	Yes	No

Table 24: IDP Support (*continued*)

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
IDP signature database	Yes	Yes	Yes	Yes
IDP SSL inspection	No	No	Yes	No
IPS rule base	Yes	Yes	Yes	Yes
Nested application identification (Extended application identification)	No	No	Yes	No
Performance and capacity tuning for IDP	No	No	Yes	No
SNMP MIB for IDP monitoring	Yes	Yes	Yes	Yes

Related Documentation • [Junos OS Security Configuration Guide](#)

IP Security

IP Security (IPsec) is a suite of related protocols for cryptographically securing communications at the IP Layer. IPsec also provides methods for the manual and automatic negotiation of security associations (SAs) and key distribution, all the attributes for which are gathered in a domain of interpretation (DOI). The IPsec DOI is a document containing definitions for all the security parameters required for successful negotiation of a VPN tunnel—essentially, all the attributes required for SA and Internet Key Exchange (IKE) negotiations.

Table 25 on page 29 lists IPsec features that are supported on SRX Series and J Series devices.

Table 25: IPsec Support

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
AH protocol	Yes	Yes	Yes	Yes
Alarms and auditing	Yes	Yes	No	No

Table 25: IPsec Support (*continued*)

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Antireplay (packet replay attack prevention)	Yes	Yes	Yes	Yes
Autokey management	Yes	Yes	Yes	Yes
Dead Peer Detection (DPD)	Yes	Yes	Yes	Yes
Dynamic IPsec VPNs	Yes	Yes	No	No
External Extended Authentication (Xauth) to a RADIUS server for remote access connections	Yes	Yes	Yes	Yes
Group VPN with dynamic policies	Yes	Yes	No	Yes
IKEv1	Yes	Yes	Yes	Yes
Manual key management	Yes	Yes	Yes	Yes
Policy-based and route-based VPNs	Yes	Yes	Yes	Yes
Tunnel mode	Yes	Yes	Yes	Yes
UAC Layer 3 enforcement	Yes	Yes	Yes	Yes
VPN monitoring (proprietary)	Yes	Yes	Yes	Yes

Related Documentation • [Junos OS Security Configuration Guide](#)

IPv6 Support

IPv6 is the successor to IPv4. IPv6 builds upon the functionality of IPv4, providing improvements to addressing, configuration and maintenance, and security. These improvements include:

- Expanded addressing capabilities—IPv6 provides a larger address space. IPv6 addresses consist of 128 bits, whereas IPv4 addresses consist of 32 bits.
- Header format simplification—The IPv6 packet header format is designed to be efficient. IPv6 standardizes the size of the packet header to 40 bytes, divided into 8 fields.
- Improved support for extensions and options—Extension headers carry Internet-layer information and have a standard size and structure.
- Improved privacy and security—IPv6 supports extensions for authentication and data integrity, which enhance privacy and security.

Table 26 on page 31 lists the SRX Series and J Series device features that support IPv6.

Table 26: IPv6 Support

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
IPv6 address configuration				
Address books	Yes	Yes	Yes	Yes
Interfaces	Yes	Yes	Yes	Yes
Security policy rule matching	Yes	Yes	Yes	Yes
IPv6 address reporting				
CLI show commands	Yes	Yes	Yes	Yes
Logging	Yes	Yes	Yes	Yes
SNMP MIB	Yes	Yes	Yes	Yes
IPv6 IDP				
Application Identification	No	No	Yes	No
IDP detector (attack detection and flow)	No	No	Yes	No
IDP in an active/active chassis cluster	No	No	Yes	No

Table 26: IPv6 Support (*continued*)

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
IDP logging	No	No	Yes	No
IDP signature database	No	No	Yes	No
Packet-based forwarding and security features				
Class of service	Yes	Yes	Yes	Yes
Firewall filters	Yes	Yes	Yes	Yes
Forwarding option: packet mode	Yes	Yes	No	Yes
Flow-based forwarding and security features				
Advanced flow	Yes	Yes	Yes	Yes
DS-lite concentrator (aka AFTR)	No	Yes	Yes	No
DS-lite initiator (aka B4)	No	No	No	No
Firewall filters	Yes	Yes	Yes	Yes
Forwarding option: flow mode	Yes	Yes	Yes	Yes
Multicast flow	Yes	Yes	Yes	Yes
Screens	Yes	Yes	Yes	Yes
Security policy (firewall)	Yes	Yes	Yes	Yes
Security policy (IDP)	Yes	No	Yes	No
Zones	Yes	Yes	Yes	Yes
Chassis cluster				
Active-active	Yes	Yes	Yes	Yes
Active-passive	Yes	Yes	Yes	Yes
Multicast flow	Yes	Yes	Yes	Yes

Table 26: IPv6 Support (*continued*)

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
IPv6 ALG Support for FTP Routing, NAT, NAT-PT support	Yes	Yes	Yes	Yes
IPv6 ALG Support for ICMP Routing, NAT, NAT-PT support	Yes	Yes	Yes	Yes
IPv6 NAT NAT-PT, NAT support	Yes	Yes	Yes	Yes
IPv6 NAT64	Yes	Yes	Yes	Yes
IPv6-related protocols BFD, BGP, ECMPv6, ICMPv6, ND, OSPFv3, RIPng	Yes	Yes	Yes	Yes
IPv6 ALG support for TFTP	Yes	Yes	Yes	Yes
System services DHCPv6, DNS, FTP, HTTP, ping, SNMP, SSH, syslog, Telnet, traceroute	Yes	Yes	Yes	Yes

Related Documentation • [Junos OS Security Configuration Guide](#)

IPv6 IP Security

IPv6 IP Security (IPsec) is the implementation of the IPsec suite of protocols in IPv6 networks.

Table 27 on page 34 lists the IPv6 IPsec features that are supported on the SRX Series and J Series devices.

Table 27: IPv6 IP Security Support

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
4in4 and 6in6 policy-based site-to-site VPN, AutoKey IKEv1	SRX100, SRX210, and SRX240 only	Yes	No	Yes
4in4 and 6in6 policy-based site-to-site VPN, manual key	SRX100, SRX210, and SRX240 only	Yes	No	Yes
4in4 and 6in6 route-based site-to-site VPN, AutoKey IKEv1	SRX100, SRX210, and SRX240 only	Yes	No	Yes
4in4 and 6in6 route-based site-to-site VPN, manual key	SRX100, SRX210, and SRX240 only	Yes	No	Yes
IKEv1 authentication, preshared key	SRX100, SRX210, and SRX240 only	Yes	No	Yes

Related Documentation • [Junos OS Security Configuration Guide](#)

Junos OS Feature Licenses

Each feature license is tied to exactly one software feature, and that license is valid for exactly one device. Table 28 on page 34 describes the Junos OS features that require licenses.

Table 28: Junos OS Feature Licenses

Junos OS License Requirements	Device								
	J Series	SRX100	SRX210	SRX220	SRX240	SRX650	SRX1000 line	SRX3000 line	SRX5000 line
Access Manager			X		X				
BGP Route Reflectors	X		X		X	X			
Dynamic VPN		X	X	X	X	X			

Table 28: Junos OS Feature Licenses (*continued*)

Junos OS License Requirements	Device								
	J Series	SRX100	SRX210	SRX220	SRX240	SRX650	SRX1000 line	SRX3000 line	SRX5000 line
IDP Signature Update	X	X *	X *	X *	X *	X	X	X	X
Application Signature Update (Application Identification)							X	X	X
Juniper-Kaspersky Anti-Virus	X	X	X	X	X	X			
Juniper-Sophos Anti-Spam	X	X	X	X	X	X			
Juniper-WebSense Integrated Web Filtering	X	X	X	X	X	X			
SRX100 Memory Upgrade		X							
UTM	X		X *		X *	X			

* Indicates support on high-memory devices only

Related Documentation

- [Junos OS Security Configuration Guide](#)
- [Junos OS Initial Configuration Guide for Security Devices](#)

Layer 2 Mode

Ethernet frames can be forwarded from one LAN segment or VLAN to another by bridging or switching functions on Juniper Networks devices. Bridging and switching functions are performed in Layer 2 of the Open Systems Interconnection (OSI) reference model—the Data Link Layer. Though the terms *bridging* and *switching* are often used interchangeably, switching functions are typically performed in hardware in application-specific integrated circuits (ASICs) while bridging functions are usually performed in software.

Table 29 on page 35 lists the Layer 2 features that are supported on SRX Series and J Series devices.

Table 29: Layer 2 Mode Support

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
802.1x port-based network authentication	Yes	Yes	No	Yes

Table 29: Layer 2 Mode Support (*continued*)

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Flexible Ethernet services	Yes	Yes	No	Yes
Generic VLAN registration protocol	Yes	Yes	No	Yes
IGMP snooping	SRX210, SRX220, and SRX240 only	Yes	No	Yes
IRB	Yes	Yes	No*	Yes
IRB interface	Yes	Yes	Yes*	Yes
LLDP and LLDP-MED	Yes	Yes	No	Yes
MAC limit (Port Security)	Yes	Yes	No	No
Q-in-Q tunneling	SRX210, SRX220, and SRX240 only	Yes	No	Yes
Spanning Tree protocols	Yes <small>NOTE: MSTP is not supported on SRX210 or SRX220.</small>	Yes	No	Yes
VLAN retagging	Yes	Yes	Yes	No
VLANs	Yes	Yes	Yes	Yes

* On SRX1400, SRX3400, SRX3600, SRX5600, and SRX5800 devices, we support an IRB interface that allows you to terminate management connections in transparent mode. However, you cannot route traffic on that interface or terminate IPsec VPNs.

Related Documentation

- [Junos OS Layer 2 Bridging and Switching Configuration Guide for Security Devices](#)

Logical Systems

Logical systems enable you to partition a single device into multiple secure logical routers, each with its own discrete administrative domain, logical interfaces, routing instances, security firewall and other security features.

Table 30 on page 37 lists features of logical systems that are supported on SRX Series devices.

Table 30: Logical Systems Support

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Administration	No	No	SRX3400, SRX3600, SRX5600, and SRX5800 only	No
Application identification	No	No	SRX3400, SRX3600, SRX5600, and SRX5800 only	No
Application tracking	No	No	SRX3400, SRX3600, SRX5600, and SRX5800 only	No
Chassis cluster	No	No	SRX3400, SRX3600, SRX5600, and SRX5800 only	No
Firewall authentication	No	No	SRX3400, SRX3600, SRX5600, and SRX5800 only	No
Interfaces	No	No	SRX3400, SRX3600, SRX5600, and SRX5800 only	No
Licensing	No	No	SRX3400, SRX3600, SRX5600, and SRX5800 only	No
Network address translation	No	No	SRX3400, SRX3600, SRX5600, and SRX5800 only	No
Routing, dynamic and static	No	No	SRX3400, SRX3600, SRX5600, and SRX5800 only	No
Screen options	No	No	SRX3400, SRX3600, SRX5600, and SRX5800 only	No
Security policies	No	No	SRX3400, SRX3600, SRX5600, and SRX5800 only	No

Table 30: Logical Systems Support (*continued*)

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Security profiles	No	No	SRX3400, SRX3600, SRX5600, and SRX5800 only	No
Sessions	No	No	SRX3400, SRX3600, SRX5600, and SRX5800 only	No
Zones	No	No	SRX3400, SRX3600, SRX5600, and SRX5800 only	No

Related Documentation • [Junos OS Logical Systems Configuration Guide for Security Devices](#)

Management

The Network Time Protocol (NTP) provides the mechanisms for synchronizing time and coordinating time distribution in a large, diverse network. NTP uses a returnable-time design in which a distributed subnet of time servers operating in a self-organizing, hierarchical primary-secondary configuration synchronizes local clocks within the subnet and to national time standards by means of wire or radio. The servers also can redistribute reference time using local routing algorithms and time daemons.

Table 31 on page 38 lists the management features that are supported on SRX Series and J Series devices.

Table 31: Management Feature Support

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
NTP	Yes	Yes	Yes	Yes

Related Documentation • [Junos OS System Basics Configuration Guide](#)

MPLS

MPLS provides a framework for controlling traffic patterns across a network. The MPLS framework allows SRX Series and J Series devices to pass traffic through transit networks

on paths that are independent of the individual routing protocols enabled throughout the network.

The MPLS framework supports traffic engineering and the creation of virtual private networks (VPNs). Traffic is engineered (controlled) primarily by the use of signaling protocols to establish label-switched paths (LSPs). VPN support includes Layer 2 and Layer 3 VPNs and Layer 2 circuits.

Table 32 on page 39 lists the MPLS features that are supported on SRX Series and J Series devices.

Table 32: MPLS Feature Support

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
CCC and TCC	Yes	Yes	No	Yes
CLNS	Yes	Yes	No	Yes
Interprovider and carrier-of-carriers VPNs	Yes	Yes	No	Yes
Layer 2 VPNs for Ethernet connections	Yes	Yes	No	Yes
Layer 3 MPLS VPNs	Yes	Yes	No	Yes
LDP	Yes	Yes	No	Yes
MPLS VPNs with VRF tables on provider edge routers	Yes	Yes	No	Yes
Multicast VPNs	Yes	No	No	Yes
OSPF and IS-IS traffic engineering extensions	Yes	Yes	No	Yes
P2MP LSPs	Yes	Yes	No	Yes
RSVP	Yes	Yes	No	Yes
Secondary and standby LSPs	Yes	Yes	No	Yes
Standards-based fast reroute	Yes	Yes	No	Yes
VPLS	Yes	Yes	No	Yes

Related Documentation • [Junos OS MPLS Configuration Guide for Security Devices](#)

Multicast

Multicast traffic lies between the extremes of unicast (one source, one destination) and broadcast (one source, all destinations). Multicast is a “one source, many destinations” method of traffic distribution, meaning that only the destinations needing to receive the information from a particular source receive the traffic stream.

IP network destinations (clients) do not often communicate directly with sources (servers), so the routers between source and destination must be able to determine the topology of the network from the unicast or multicast perspective to avoid routing traffic haphazardly. The multicast router must find multicast sources on the network, send out copies of packets on several interfaces, prevent routing loops, connect interested destinations with the proper source, and keep the flow of unwanted packets to a minimum. Standard multicast routing protocols provide most of these capabilities.

Table 33 on page 40 lists the multicast features that are supported on SRX Series and J Series devices.

Table 33: Multicast Support

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Filtering PIM register messages	Yes	Yes	Yes	Yes
IGMP	Yes	Yes	Yes	Yes
PIM RPF Routing Table	Yes	Yes	Yes	Yes
Primary routing mode (dense mode for LAN and sparse mode for WAN)	Yes	Yes	Yes	Yes
Protocol Independent Multicast Static RP	Yes	Yes	Yes	Yes
Session Announcement Protocol (SAP)	Yes	Yes	Yes	Yes
SDP	Yes	Yes	Yes	Yes

Related Documentation • [Junos OS Interfaces Configuration Guide for Security Devices](#)

Multicast VPN

MPLS multicast VPNs employ the intra-autonomous system (AS) next-generation (NGEN) BGP control plane and Protocol Independent Multicast (PIM) sparse mode as the data plane.

A multicast VPN is defined by two sets of sites, a sender site set and a receiver site set. These sites have the following properties:

- Hosts within the sender site set can originate multicast traffic for receivers in the receiver site set.
- Receivers outside the receiver site set should not be able to receive this traffic.
- Hosts within the receiver site set can receive multicast traffic originated by any host in the sender site set.
- Hosts within the receiver site set should not be able to receive multicast traffic originated by any host that is not in the sender site set.

Table 34 on page 41 lists the multicast VPN features that are supported on J Series devices.

Table 34: Multicast VPN Support

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Basic multicast features in C-instance	No	No	No	Yes
Multicast VPN membership discovery with BGP	No	No	No	Yes
P2MP LSP support	No	No	No	Yes
P2MP OAM - P2MP LSP ping	No	No	No	Yes
Reliable multicast VPN routing information exchange	No	No	No	Yes

Related Documentation • [Junos OS VPNs Configuration Guide](#)

Network Address Translation

Network Address Translation (NAT) is a method by which IP addresses in a packet are mapped from one group to another and, optionally, port numbers in the packet are translated into different port numbers.

NAT is described in RFC 3022 to solve IP (version 4) address depletion problems. Since then, NAT has been found to be a useful tool for firewalls, traffic redirect, load sharing, network migrations, and so on.

Table 35 on page 42 lists NAT features that are supported on SRX Series and J Series devices.

Table 35: NAT Support

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Destination IP address translation	Yes	Yes	Yes	Yes
Disabling source NAT port randomization	Yes	Yes	Yes	Yes
Interface source NAT pool port	Yes	Yes	Yes	Yes
NAT address pool utilization threshold status	Yes	Yes	Yes	Yes
Persistent NAT	Yes	Yes	Yes	Yes
Persistent NAT Hairpinning	Yes	Yes	Yes	Yes
Persistent NAT binding for wildcard ports	Yes	Yes	Yes	Yes
Pool translation	Yes	Yes	Yes	Yes
Proxy ARP	Yes	Yes	Yes	Yes
Removing persistent NAT query bindings	Yes	Yes	Yes	Yes
Rule-based NAT	Yes	Yes	Yes	Yes
Rule translation	Yes	Yes	Yes	Yes

Table 35: NAT Support (*continued*)

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Source address and group address translation for multicast flows	Yes	Yes	Yes	Yes
Source IP address translation	Yes	Yes	Yes	Yes
Static NAT	Yes	Yes	Yes	Yes

Related Documentation • [Junos OS Security Configuration Guide](#)

Network Operations and Troubleshooting

You can use commit scripts, operation scripts, and event policies to automate network operations and troubleshooting tasks. You can use commit scripts to enforce custom configuration rules. You can use operation scripts to automate network management and troubleshooting tasks. You can configure event policies that initiate self-diagnostic actions on the occurrence of specific events.

Table 36 on page 43 lists the network operations features that are supported on SRX Series and J Series devices.

Table 36: Network Operations and Troubleshooting Support

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Event policies	Yes	Yes	Yes	Yes
Event scripts	Yes	Yes	Yes	Yes
Operation scripts	Yes	Yes	Yes	Yes
XSLT commit scripts	Yes	Yes	Yes	Yes

Related Documentation • [Junos OS Monitoring and Troubleshooting Guide for Security Devices](#)

Packet Capture

Packet capture is a tool that helps you analyze network traffic and troubleshoot network problems. The packet capture tool captures real-time data packets, traveling over the network, for monitoring and logging.



NOTE: *Packet capture*, in this context, refers to standard interface packet capture. It is not part of the IDP. Packet capture is supported only on physical interfaces and tunnel interfaces; for example, *gr*, *ip*, *st0*, *lsq-/ls-*. Packet capture is not supported on redundant Ethernet interfaces (*reth*).

Packets are captured as binary data, without modification. You can read the packet information offline with a packet analyzer such as Ethereal or tcpdump.

Table 37 on page 44 lists the packet capture support on SRX Series and J Series devices.

Table 37: Packet Capture Support

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Packet capture	Yes	Yes	Yes	Yes

Related Documentation

- [Junos OS Monitoring and Troubleshooting Guide for Security Devices](#)

Power over Ethernet

Power over Ethernet (PoE) is the implementation of the IEEE 802.3 AF standard, which allows both data and electrical power to pass over a copper Ethernet LAN cable.

PoE ports transfer electrical power and data to remote devices over standard twisted-pair cable in an Ethernet network. PoE ports allow you to plug in devices that require both network connectivity and electrical power, such as voice over IP (VoIP) and IP phones and wireless LAN access points.

Table 38 on page 45 lists the PoE support on SRX Series and J Series devices.

Table 38: PoE Support

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
IEEE 802.3 AF standard	SRX210 (PoE), SRX220 (PoE model), and SRX240 (PoE)	Yes	No	No
IEEE 802.3 AT standard	SRX210 SRX220, and SRX240 only	Yes	No	No
IEEE legacy (pre-standards)	SRX210 SRX220, and SRX240 only	Yes	No	No

Related Documentation • [Junos OS Interfaces Configuration Guide for Security Devices](#)

Public Key Infrastructure

In Public Key Infrastructure (PKI), a public-private key pair is used to encrypt and decrypt data. Data encrypted with a public key, which the owner makes available to the public, can be decrypted with the corresponding private key only, which the owner keeps secret and protected.

The reverse process is also useful: encrypting data with a private key and decrypting it with the corresponding public key. This process is known as creating a digital signature. A *digital certificate* is an electronic means for verifying your identity through a trusted third party, known as a certificate authority (CA).

Table 39 on page 45 lists the PKI features that are supported on SRX Series and J Series devices.

Table 39: PKI Support

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Automated certificate enrollment using SCEP	Yes	Yes	Yes	Yes
Automatic generation of self-signed certificates	Yes	Yes	Yes	Yes
CRL update at user-specified interval	Yes	Yes	Yes	Yes

Table 39: PKI Support (*continued*)

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
DERs, PEM, PKCS7, and X509 certificate encoding	Yes	Yes	Yes	Yes
Digital signature generation	Yes	Yes	SRX3400, SRX3600, SRX5600, and SRX5800 only	Yes
Entrust, Microsoft, and Verisign certificate authorities (CAs)	Yes	Yes	Yes	Yes
IKE Diffie-Hellman Group 14 support	Yes	Yes	SRX3400, SRX3600, SRX5600, and SRX5800 only	Yes
IKE support	Yes	Yes	Yes	Yes
Manual installation of DER-encoded and PEM-encoded CRLs	Yes	Yes	Yes	Yes
Online CRL retrieval through LDAP and HTTP	Yes	Yes	Yes	Yes

Related Documentation • [Junos OS Security Configuration Guide](#)

Real-Time Performance Monitoring Probe

The real-time performance monitoring (RPM) feature allows network operators and their customers to accurately measure the performance between two network endpoints. With the RPM probe, you configure and send probes to a specified target and monitor the analyzed results to determine packet loss, round-trip time, and jitter.

Table 40 on page 47 lists the RPM probe support on SRX Series and J Series devices.

Table 40: RPM Probe Support

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
RPM probe	Yes	Yes	No	Yes

Related Documentation • [Junos OS Monitoring and Troubleshooting Guide for Security Devices](#)

Remote Device Access

You can use the CLI telnet command to open a Telnet session to a remote device.

Table 41 on page 47 lists the remote device access support on SRX Series and J Series devices.

Table 41: Remote Device Access Support

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Reverse Telnet	No	Yes	Yes	Yes

Related Documentation • [Junos OS Initial Configuration Guide for Security Devices](#)

Routing

Routing is the transmission of data packets from a source to a destination address. For packets to be correctly forwarded to the appropriate host address, the host must have a unique numeric identifier or IP address. The unique IP address of the destination host forms entries in the routing table. These entries are primarily responsible for determining the path that a packet traverses when transmitted from source to destination.

Table 42 on page 47 lists the routing features that are supported on SRX Series and J Series devices.

Table 42: Routing Support

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
BGP	Yes	Yes	No	Yes

Table 42: Routing Support (continued)

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
BGP extensions for IPv6	Yes	Yes	Yes	Yes
Compressed Real-Time Transport Protocol (CRTP)	Yes	No	No	Yes
Internet Group Management Protocol (IGMP)	Yes	Yes	Yes	Yes
IPv4 options and broadcast Internet diagrams	Yes	Yes	Yes	Yes
IPv6 routing, forwarding, global address configuration, and Internet Control Message Protocol (ICMP)	Yes	Yes	Yes	Yes
IS-IS	Yes	Yes	Yes	Yes
Multiple virtual routers	Yes	Yes	Yes	Yes
Neighbor Discovery Protocol and Secure Neighbor Discovery Protocol	Yes	Yes	Yes	Yes
OSPF v2	Yes	Yes	Yes	Yes
OSPF v3	Yes	Yes	Yes	Yes
RIP next generation (RIPng)	Yes	Yes	Yes	Yes
RIP v1, v2	Yes	Yes	Yes	Yes
Static routing	Yes	Yes	Yes	Yes
Virtual Router Redundancy Protocol (VRRP)	Yes	Yes	Yes	Yes

Related Documentation • [Junos OS Routing Protocols and Policies Configuration Guide for Security Devices](#)

Secure Web Access

You can manage a Juniper Networks device remotely through the J-Web interface. To communicate with the device, the J-Web interface uses Hypertext Transfer Protocol (HTTP). HTTP allows easy Web access but no encryption. The data that is transmitted between the Web browser and the device by means of HTTP is vulnerable to interception and attack. To enable secure Web access, the Juniper Networks devices support Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS). You can enable HTTP or HTTPS access on specific interfaces and ports as needed.

Table 43 on page 49 lists the secure web access features that are supported on SRX Series and J Series devices.

Table 43: Secure Web Access Support

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
CAs	Yes	Yes	Yes	Yes
HTTP	Yes	Yes	Yes	Yes
HTTPS	Yes	Yes	Yes	Yes

Related Documentation • [Junos OS Initial Configuration Guide for Security Devices](#)

Security Policy

With the advent of the Internet, the need for a secure network has become vital for businesses with an Internet connection. Before a network can be secured for a business, a network security policy has to outline all the network resources within that business and identify the required security level for those resources. The network security policy also defines the security threats and the actions taken for such threats. Junos OS stateful firewall policy provides a set of tools to network administrators, enabling them to implement network security for their organizations.

Table 44 on page 50 lists the security policy features that are supported on SRX Series and J Series devices.

Table 44: Security Policy Support

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Address books	Yes	Yes	Yes	Yes
Custom policy applications	Yes	Yes	Yes	Yes
Dynamic routing protocols predefined policy applications	Yes	Yes	Yes	Yes
ICMP predefined policy application	Yes	Yes	Yes	Yes
Instant messaging predefined policy applications	Yes	Yes	Yes	Yes
Internet-related predefined policy applications	Yes	Yes	Yes	Yes
IP-related predefined policy applications	Yes	Yes	Yes	Yes
Mail predefined policy applications	Yes	Yes	Yes	Yes
Management predefined policy applications	Yes	Yes	Yes	Yes
Microsoft predefined policy applications	Yes	Yes	Yes	Yes
Miscellaneous predefined policy applications	Yes	Yes	Yes	Yes
Policy application timeouts	Yes	Yes	Yes	Yes
Policy applications and application sets	Yes	Yes	Yes	Yes
Schedulers	Yes	Yes	Yes	Yes

Table 44: Security Policy Support (*continued*)

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Security and tunnel predefined policy applications	Yes	Yes	Yes	Yes
Streaming video predefined policy applications	Yes	Yes	Yes	Yes
SUN RPC predefined policy applications	Yes	Yes	Yes	Yes
UNIX predefined policy applications	Yes	Yes	Yes	Yes

Related Documentation • [Junos OS Security Configuration Guide](#)

Security Zone

A *security zone* is a collection of one or more network segments requiring the regulation of inbound and outbound traffic through policies. Security zones are logical entities to which one or more interfaces are bound. On a single device, you can configure multiple security zones, dividing the network into segments to which you can apply various security options to satisfy the needs of each segment. At a minimum, you must define two security zones, basically to protect one area of the network from the other.

Junos OS supports the following two types of zones:

- Functional zones
- Security zones

Table 45 on page 51 lists the zones supported on SRX Series and J Series devices.

Table 45: Zones Support

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Functional zone	Yes	Yes	Yes	Yes
Security zone	Yes	Yes	Yes	Yes

Related Documentation • [Junos OS Security Configuration Guide](#)

Session Logging

You can obtain information about the sessions and packet flows active on your device, including detailed information about specific sessions. (The SRX Series device also displays information about failed sessions.) You can display this information to observe activity and for debugging purposes.

Table 46 on page 52 lists the session logging features that are supported on SRX Series and J Series devices.

Table 46: Session Logging Support

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Accelerating security and traffic logging	Yes	Yes	Yes	Yes
Getting information about sessions	Yes	Yes	Yes	Yes
Logging to a single server	Yes	Yes	Yes	Yes
Session logging with NAT information	Yes	Yes	Yes	Yes

Related Documentation • [Junos OS Security Configuration Guide](#)

SMTP

Use SMTP to send an e-mail message to a local or a remote mail server to forward an e-mail message.

Table 47 on page 52 lists the SRX Series and J Series devices that support SMTP.

Table 47: SMTP Support

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
SMTP	Yes	Yes	Yes	Yes

Related Documentation • [Junos OS CLI User Guide](#)

SNMP

SNMP enables the monitoring of network devices from a central location.

Use SNMP to determine where and when a network failure is occurring, and to gather statistics about network performance in order to evaluate the overall health of the network and identify bottlenecks.

Table 48 on page 53 lists the SNMP support on SRX Series and J Series devices.

Table 48: SNMP Support

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
SNMP v1, v2, v3	Yes	Yes	Yes	Yes

Related Documentation

Stateless Firewall Filters

A stateless firewall filter evaluates the contents of packets transiting the device from a source to a destination, or the contents of packets originating from, or destined for, the Routing Engine. Stateless firewall filters applied to the Routing Engine interface protect the processes and resources owned by the Routing Engine. A stateless firewall filter evaluates every packet, including fragmented packets.

A stateless firewall filter, often called a *firewall filter* or *access control list (ACL)*, statically evaluates packet contents. In contrast, a stateful firewall filter uses connection state information derived from past communications and other applications to make dynamic control decisions.

Table 49 on page 53 lists the stateless firewall filters support on SRX Series and J Series devices.

Table 49: Stateless Firewall Filters Support

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Stateless firewall filters (ACLs)	Yes	Yes	Yes	Yes

Related Documentation • [Junos OS Routing Protocols and Policies Configuration Guide for Security Devices](#)

System Log Files

Junos OS supports configuring and monitoring of system log messages (also called *syslog messages*). You can configure files to log system messages and also assign attributes, such as severity levels, to messages. The View Events page in the J-Web interface enables you to filter and view system log messages.

Table 50 on page 54 lists the system log files features that are supported on SRX Series and J Series devices.

Table 50: System Log Files Support

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Archiving system logs	Yes	Yes	Yes	Yes
Configuring system log messages	Yes	Yes	Yes	Yes
Disabling system logs	Yes	Yes	Yes	Yes
Filtering system log messages	Yes	Yes	Yes	Yes
Multiple system log servers (control-plane logs)	Yes	Yes	Yes	No
Sending system log messages to a file	Yes	Yes	Yes	Yes
Sending system log messages to a user terminal	Yes	Yes	Yes	Yes
Viewing data plane logs	Yes	Yes	Yes	Yes
Viewing system log messages	Yes	Yes	Yes	Yes

Related Documentation • [Junos OS Monitoring and Troubleshooting Guide for Security Devices](#)

Transparent Mode

In transparent mode, the SRX Series device filters packets that traverse the device without modifying any of the source or destination information in the IP packet headers. Transparent mode is useful for protecting servers that mainly receive traffic from untrusted sources because there is no need to reconfigure the IP settings of routers or protected servers.

Table 51 on page 55 lists the transparent mode features that are supported on SRX Series devices.

Table 51: Transparent Mode Support

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Bridge domain and transparent mode	Yes	Yes	Yes	No
Chassis clusters (active/backup and active/active)	Yes	Yes	Yes	No
Class of service	Yes	Yes	Yes	No

Related Documentation • [Junos OS Layer 2 Bridging and Switching Configuration Guide for Security Devices](#)

Unified Threat Management

Unified Threat Management (UTM) is a term used to describe the consolidation of several security features into one device, protecting against multiple threat types. The advantages of UTM are streamlined installation and management of these multiple security capabilities.

Table 52 on page 55 lists the UTM features that are supported on SRX Series and J Series devices.

Table 52: UTM Support

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Antispam	Yes	Yes	No	Yes
Antivirus Express	Yes	Yes	No	Yes

Table 52: UTM Support (*continued*)

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Antivirus Full	Yes	Yes	No	Yes
Antivirus Sophos	Yes	Yes	No	No
Content filtering	Yes	Yes	No	Yes
Web filtering	Yes	Yes	No	Yes
WELF support	Yes	Yes	No	Yes

Related Documentation • [Junos OS Security Configuration Guide](#)

Upgrading and Rebooting

J Series and SRX Series devices are delivered with Junos OS preinstalled. When you power on the device, it starts (boots) up using its primary boot device. These devices also support secondary boot devices, allowing you to back up your primary boot device and configuration.

As new features and software fixes become available, you must upgrade your software to use them. Before an upgrade, we recommend that you back up your primary boot device.

You can configure the primary or secondary boot device with a snapshot of the current configuration, default factory configuration, or rescue configuration. You can also replicate the configuration for use on another device, or configure a boot device to receive core dumps for troubleshooting.

Table 53 on page 56 lists the upgrading and rebooting features that are supported on SRX Series and J Series devices.

Table 53: Upgrading and Rebooting Support

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Boot device configuration	Yes	Yes	Yes	Yes
Boot device recovery	Yes	Yes	Yes	Yes

Table 53: Upgrading and Rebooting Support (*continued*)

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Chassis components control	Yes	Yes	Yes	Yes
Chassis restart	Yes	Yes	Yes	Yes
Dual-root partitioning	Yes	Yes	No	Yes
Low-impact cluster upgrades	No	No	Yes	No
Software upgrades and downgrades	Yes	Yes	Yes	Yes

Related Documentation • [Junos OS Initial Configuration Guide for Security Devices](#)

USB Modem

SRX Series devices support the use of USB modems for remote management. You can use Telnet or SSH to connect to the device from a remote location through two modems over a telephone network. The USB modem is connected to the USB port on the device, and a second modem is connected to a remote management device such as a PC or laptop computer.

Table 54 on page 57 lists the USB modem support for SRX Series devices.

Table 54: USB Modem Support

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
USB modem support	Yes	Yes	Yes	No

Related Documentation • [Junos OS Initial Configuration Guide for Security Devices](#)

User Interfaces

You can use two user interfaces to monitor, configure, troubleshoot, and manage your device—the J-Web interface and the command-line interface (CLI) for Junos OS.

Table 55 on page 58 lists the user interface features that are supported on SRX Series and J Series devices.

Table 55: User Interfaces Support

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
CLI	Yes	Yes	Yes	Yes
J-Web user interface	Yes	Yes	Yes	Yes
Junos XML protocol	Yes	Yes	Yes	Yes
Network and Security Manager	Yes	Yes	Yes	Yes
SRC application	No	Yes	No	Yes

Related Documentation • [Junos OS Initial Configuration Guide for Security Devices](#)

Voice over Internet Protocol with Avaya

J2320, J2350, J4350, and J6350 Services Routers support voice over IP (VoIP) connectivity for branch offices with the Avaya IG550 Integrated Gateway. The Avaya IG550 Integrated Gateway consists of four VoIP modules—a TGM550 Telephony Gateway Module and three types of Telephony Interface Modules (TIMs).

Table 56 on page 58 lists the VoIP with Avaya features that are supported only on J Series devices.

Table 56: VoIP with Avaya Support

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Avaya Communication Manager	No	No	No	Yes

Table 56: VoIP with Avaya Support (continued)

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Avaya VoIP Modules:	No	No	No	Yes
<ul style="list-style-type: none"> • TGM550 Telephony Gateway Module • TIM508 Analog Telephony Interface Module • TIM510 E1/T1 Telephony Interface Module • TIM514 Analog Telephony Interface Module • TIM516 Analog Telephony Interface Module • TIM518 Analog Telephony Interface Module • TIM521 BRI Telephony Interface Module 				
Dynamic Call Admission Control	No	No	No	Yes
Media Gateway Controller	No	No	No	Yes
VoIP interfaces:	No	No	No	Yes
<ul style="list-style-type: none"> • Analog telephone or trunk port • E1 port • ISDN BRI telephone or trunk port • T1 port 				

Related Documentation • [Junos OS Interfaces Configuration Guide for Security Devices](#)

Wireless Local Area Network

A wireless local area network (WLAN) implements a flexible data communication system that frequently augments rather than replaces a wired LAN within a building, thus minimizing the need for wired connections.

Table 57 on page 60 lists the WLAN support on SRX Series and J Series devices.

Table 57: Wireless LAN Support

Feature	SRX100 SRX210 SRX220 SRX240	SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Wireless LAN	SRX210, SRX220, and SRX240 only	Yes	No	No



NOTE: The maximum number of AX411 Access Points supported on an SRX Series Services Gateway is device dependent. Please see the release notes.

- Related Documentation**
- [Junos OS WLAN Configuration and Administration Guide](#)

PART 2

Index

- Index on page 63

Index

Symbols

#, comments in configuration statements.....	xi
(), in syntax descriptions.....	xi
< >, in syntax descriptions.....	xi
[], in configuration statements.....	xi
{ }, in configuration statements.....	xi
(pipe), in syntax descriptions.....	xi

A

Access Manager license.....	34
address book.....	6
support table.....	6
administrator authentication.....	7
support table.....	7
alarms.....	8
support tables.....	8
ALG See Application Layer Gateway	
application identification.....	9
support table.....	9
Application Layer Gateway.....	9
support table.....	9
autoinstallation.....	13
support table.....	13

B

BGP route reflectors license.....	34
Border Gateway Protocol (BGP) route reflectors	
license.....	34
braces, in configuration statements.....	xi
brackets	
angle, in syntax descriptions.....	xi
square, in configuration statements.....	xi

C

chassis cluster.....	13
support table.....	13
chassis management.....	15
support table.....	15
class of service.....	16
support table.....	16

comments, in configuration statements.....	xi
conventions	
notice icons.....	x
text and syntax.....	x
CoS See class of service	
curly braces, in configuration statements.....	xi
customer support.....	xii
contacting JTAC.....	xii

D

device access	
remote.....	47
DHCP See Dynamic Host Configuration Protocol	
documentation	
comments on.....	xi
Dynamic Host Configuration Protocol.....	17
support table.....	17
Dynamic VPN	
support table.....	18
Dynamic VPN license.....	34

E

Ethernet link aggregation.....	19
support table.....	19

F

file management.....	20
support table.....	20
firewall authentication.....	20
support table.....	20
firewall filters	
stateless.....	53
flow-based and packet-based processing.....	21
support table.....	21
font conventions.....	x

G

General Packet Radio Service.....	22
support table.....	22
GPRS See General Packet Radio Service	

H

hardware	
supported platforms.....	ix

I

IDP signature update license.....	34
infranet authentication.....	12
support table.....	12
interfaces.....	23
support table.....	23
user.....	57
Intrusion Detection and Prevention.....	27
support table.....	27
Intrusion Detection and Prevention (IDP) signature update license.....	34
IPsec.....	29
support table.....	29
IPv6.....	31, 33
support table.....	31
IPv6 IP Security	
support table.....	33

J

J Series Services Devices	
licenses.....	34
Juniper-Kaspersky Anti-Virus license.....	34
Juniper-Sophos Anti-Spam license.....	34
Juniper-WebSense Integrated Web Filtering license.....	34

L

Layer 2 mode.....	35, 38
support table.....	35
licenses	
Access Manager.....	34
application signature update (Application Identification).....	34
BGP route reflectors.....	34
Dynamic VPN.....	34
IDP signature update.....	34
J Series Services Device	34
Juniper-Kaspersky Anti-Virus.....	34
Juniper-Sophos Anti-Spam.....	34
Juniper-WebSense Integrated Web Filtering license.....	34
SRX Series Services Gateway.....	34
SRX100 Memory Upgrade license.....	34
UTM.....	34

logging	
sessions.....	52
logical systems.....	36
support table.....	36

M

management.....	38
support table.....	38
manuals	
comments on.....	xi
mode	
Layer 2.....	35
transparent.....	55
modem	
USB.....	57
MPLS.....	38
multicast.....	40
support table.....	40
multicast VPN.....	41

N

NAT See Network Address Translation	
Network Address Translation.....	42
support table.....	42
network operations and troubleshooting.....	43
support table.....	43
notice icons.....	x
NTP See management	

P

packet capture.....	44
support table.....	44
See also flow-based and packet-based processing	
parentheses, in syntax descriptions.....	xi
PKI See Public Key Infrastructure	
PoE See Power over Ethernet	
policy	
security.....	49
Power over Ethernet.....	44
support table.....	44
Public Key Infrastructure.....	45
support table.....	45

R

real-time performance monitoring probe.....	46
support table.....	46
remote device access.....	47
support table.....	47

route reflectors, BGP, license.....	34	Voice over Internet Protocol.....	58
routing.....	47	support table.....	58
support table.....	47	VoIP See Voice over Internet Protocol	
RPM See real-time performance monitoring probe		VPN See virtual private network	
S		multicast.....	41
secure web access.....	49	W	
support table.....	49	wireless LAN.....	59
security policy.....	49	support table.....	58
support table.....	49	WLAN See wireless LAN	
session logging.....	52	Z	
signature update, IDP, license.....	34	zones.....	51
SMTP.....	52	support table.....	51
support table.....	52		
SNMP.....	53		
support table.....	53		
SRX Series Services Gateway			
licenses.....	34		
SRX100 Memory Upgrade license.....	34		
stateless firewall filters.....	53		
support table.....	53		
support, technical See technical support			
syntax conventions.....	x		
system log files.....	54		
support table.....	54		
T			
technical support			
contacting JTAC.....	xii		
transparent mode.....	55		
troubleshooting			
feature support.....	43		
U			
Unified Threat Management.....	55		
support table.....	55		
Unified Threat Management (UTM) license.....	34		
upgrading and rebooting.....	56		
support table.....	56		
USB modem.....	57		
support table.....	57		
user interfaces.....	57		
support table.....	57		
UTM See Unified Threat Management			
UTM license.....	34		
V			
virtual private network			
multicast.....	41		

