Junos® OS

Feature Support Reference for SRX Series and J Series Devices

Release

12.1

Published: 2012-03-06

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

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

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

Junos OS Feature Support Reference for SRX Series and J Series Devices
Release 12.1
Copyright © 2012, Juniper Networks, Inc.
All rights reserved.

Revision History
March 2012—R1 Junos OS 12.1

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. 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

Table of Contents

Part 2 Index

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

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 viii defines the notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
ℹ	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 viii 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`
Italic text like this	• Introduces important new terms. • Identifies book names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS System Basics Configuration Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	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** *domain-name*

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.	- To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. - The console port is labeled **CONSOLE**.
< > (angle brackets)	Enclose optional keywords or variables.	**stub <default-metric *metric*>;**
| (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** (***string1* | *string2* | *string3***)
# (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*]**

Indention and braces ({ })	Identify a level in the configuration hierarchy.	[edit]
		routing-options {
		static {
		route default {
		nexthop *address*;
		retain;
		}
		}
		}

; (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.	- 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

CHAPTER 1

Juniper Networks Devices’ Feature Support

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
- SRX110
- SRX210
- SRX220
- SRX240
- SRX550
- 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

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 SRX110 SRX210 SRX220 SRX240	SRX550 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	Yes	Yes	Yes	Yes
Nested address groups	Yes	Yes	Yes	Yes

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 8 lists the administrator authentication features that are supported on SRX Series and J Series devices.

Table 4: Administrator Authentication Support

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Local authentication	Yes	Yes	Yes	Yes
RADIUS	Yes	Yes	Yes	Yes
TACACS+	Yes	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 SRX110 SRX210 SRX220 SRX240	SRX550 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 provides data for application tracking (AppTrack), Application Firewall (AppFW), Application QoS (AppQoS), and Application DDoS, and allows Intrusion Detection and Prevention (IDP) to apply appropriate attack objects to applications running on nonstandard ports.

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 SRX110 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Application DDoS (AppDoS)	No	No	Yes	No
Application Firewall (AppFW)	Yes	Yes	Yes	No
Application QoS (AppQoS)	No	No	Yes	No
Application Tracking (AppTrack)	Yes	Yes	Yes	No
Custom application signatures and signature groups	Yes	Yes	Yes	No
Heuristics-based detection	Yes	Yes	Yes	No
IDP	Yes	Yes	Yes	Yes
Jumbo frames	SRX210, SRX220, and SRX240 only	Yes	Yes (9192 bytes)	Yes (9010 bytes)
Nested application identification	Yes	Yes	Yes	No
Onbox application tracking statistics (AppTrack)	Yes	Yes	Yes	No
User role integration into AppTrack logs	Yes	Yes	Yes	No

Related Documentation

- Intrusion Detection and Prevention on page 30

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 SRX110 SRX210 SRX220 SRX240	SRX550 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	SRX100, SRX210, SRX220, and SRX240 only	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	Yes	Yes
Avaya H.323	Yes	Yes	Yes	Yes
IKE	Yes	Yes	Yes	No
MGCP	Yes	Yes	Yes	Yes
PPTP	Yes	Yes	Yes	Yes
RSH	Yes	Yes	Yes	Yes
RTSP	Yes	Yes	Yes	Yes
SCCP	Yes	Yes	Yes	Yes
SIP	Yes	Yes	Yes	Yes

Table 7: ALG Support *(continued)*

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
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 SRX110 SRX210 SRX220 SRX240	SRX550 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

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

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
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
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

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

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
UDP address sweep	Yes	Yes	Yes	Yes
UDP flood protection	Yes	Yes	Yes	Yes
Unknown IP protocol protection	Yes	Yes	Yes	Yes
Whitelist for SYN flood screens	Yes	Yes	Yes	Yes
WinNuke attack protection	Yes	Yes	Yes	Yes

Related Documentation

- *Junos OS Security Configuration Guide*
- Intrusion Detection and Prevention on page 30

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 SRX110 SRX210 SRX220 SRX240	SRX550 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 14 lists the autoinstallation support on SRX Series and J Series devices.

Table 10: Autoinstallation Support

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 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.

NOTE: On SRX110 devices, chassis cluster is not supported.

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	SRX550 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

Table 11: Chassis Cluster Support *(continued)*

Feature	SRX100 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
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
In-band cluster upgrade	Yes	Yes	No	No
Junos OS flow-based routing functionality	Yes	Yes	Yes	Yes
Layer 2 Ethernet switching capability	Yes	Yes	No	No
Layer 2 LAG	Yes	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
Low latency firewall	No	No	Yes	No
Multicast routing	Yes	Yes	Yes	Yes

Table 11: Chassis Cluster Support *(continued)*

Feature	SRX100 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
PPPoE over redundant Ethernet interface	Yes	Yes	No	No
Redundant Ethernet interfaces	Yes	Yes	Yes	Yes
Redundant Ethernet interface LAGs	Yes	Yes	Yes	Yes
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	Yes	Yes	Yes	No
Upstream device IP address monitoring on a backup interface	Yes	Yes	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 16 lists the chassis management support on SRX Series and J Series devices.

Table 12: Chassis Management Support

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 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 17 lists the CoS features that are supported on SRX Series and J Series devices.

Table 13: CoS Support

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 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	Yes	Yes
Forwarding classes	Yes	Yes	Yes	Yes
High-priority queue on Services Processing Card	No	No	Yes	No
Ingress interface policer	Yes	Yes	Yes	Yes
Schedulers	Yes	Yes	Yes	Yes
Simple filters	Yes	Yes	Yes	No
Transmission queues	Yes	Yes	Yes	Yes
Tunnels NOTE: GRE and IP-IP tunnels only.	Yes	Yes	Yes	Yes
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 18 lists the DHCP features that are supported on SRX Series and J Series devices.

Table 14: DHCP Support

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
DHCPv6 client	No	No	No	No
DHCPv4 client	Yes	Yes	Yes	Yes
DHCPv6 relay agent	Yes	Yes	Yes	Yes
DHCPv4 relay agent	Yes	Yes	Yes	Yes
DHCPv6 server	Yes	Yes	Yes	Yes
DHCPv4 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 19 lists the dynamic VPN features that are supported on SRX Series and J Series devices.

Table 15: Dynamic VPN Support

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Package dynamic VPN client	Yes	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 19 lists the diagnostics tools features that are supported on SRX Series and J Series devices.

Table 16: Diagnostics Tools Support

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 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 14.

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 20 lists the Ethernet link aggregation features that are supported on SRX Series and J Series devices.

Table 17: Ethernet Link Aggregation Support

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Layer 2 Transparent Mode				
LACP in a standalone device	No	No	No	No
LACP in a chassis cluster pair	SRX100, SRX210, SRX220, and SRX240 only	No	No	No
Static LAG in transparent mode	No	No	Yes	No
Routing mode				
LACP in chassis cluster pair	SRX100, SRX210, SRX220, and SRX240 only	Yes	Yes	Yes
LACP in standalone device	Yes	Yes	Yes	Yes
Layer 3 LAG on routed ports	Yes	Yes	Yes	Yes
Static LAG in chassis cluster mode	SRX100, SRX210, SRX220, and SRX240 only	Yes	Yes	Yes

Table 17: Ethernet Link Aggregation Support *(continued)*

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Static LAG in standalone mode	Yes	Yes	Yes	Yes
Switching mode				
LACP in chassis cluster pair	SRX100, SRX210, SRX220, and SRX240 only	Yes	–	No
LACP in standalone device	Yes	Yes	–	Yes
Static LAG in chassis cluster mode	SRX100, SRX210, SRX220, and SRX240 only	Yes	–	No
Static LAG 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 21 lists the file management features that are supported on SRX Series and J Series devices.

Table 18: File Management Support

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 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

Table 18: File Management Support *(continued)*

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Download system files	Yes	Yes	Yes	Yes
Encrypt/decrypt configuration files	Yes	Yes	Yes	Yes
Manage account files	Yes	Yes	No	Yes
Rescue	Yes	Yes	Yes	Yes
System snapshot	Yes	Yes	Yes	Yes
System zeroize	Yes	Yes	Yes	Yes
Monitor start	Yes	Yes	Yes	Yes
Archive files	Yes	Yes	Yes	Yes
Calculate checksum	Yes	Yes	Yes	Yes
Compare files	Yes	Yes	Yes	Yes
Rename files	Yes	Yes	Yes	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 23 lists firewall authentication features that are supported on SRX Series and J Series devices.

Table 19: Firewall Authentication Support

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 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 24 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 SRX110 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Alarms and auditing	Yes	Yes	Yes	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 25 lists GPRS features that are supported on SRX Series and J Series devices.

Table 21: GPRS Support

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Customized informational element (IE) removal	No	No	Yes	No
GPRS	No	No	Yes	No

Related Documentation

- *Junos OS Security Configuration Guide*

GTPv2

GPRS tunneling protocol version 2 (GTPv2) is part of Long Term Evolution (LTE), a fourth generation (4G) wireless broadband technology developed by the Third Generation Partnership Project (3GPP). 3GPP is the standard body for developing GPRS standards. LTE is designed to increase the capacity and speed of mobile telephone networks. GTPv2 is a protocol designed for LTE networks.

An LTE network comprises network elements, LTE interfaces, and protocols. In previous releases, only GTP version 0 (GTPv0), and GTP version 1 (GTPv1) were deployed. GTP version 2 (GTPv2) is implemented in the Junos operating system (Junos OS) Release 11.4.

Table 22 on page 25 lists the GTPv2 features supported on SRX Series and J Series devices.

Table 22: GTPv2 Support

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
IMSI prefix and APN filtering	No	No	Yes	No
Message-length filtering	No	No	Yes	No
Message-rate limiting	No	No	Yes	No
Message-type filtering	No	No	Yes	No
Packet sanity check	No	No	Yes	No

Table 22: GTPv2 Support *(continued)*

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Policy-based inspection	No	No	Yes	No
Restart GTPv2 path	No	No	Yes	No
Stateful inspection	No	No	Yes	No
Traffic logging	No	No	Yes	No
Tunnel cleanup	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 23 on page 26 lists the physical and virtual interfaces features that are supported on SRX Series and J Series devices.

Table 23: Physical and Virtual Interface Support

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
1-Port Gigabit Ethernet SFP Mini-PIM interface	Yes	SRX550 only	No	No
10-Gigabit Ethernet interface	No	Yes	Yes	No

Table 23: Physical and Virtual Interface Support *(continued)*

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
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
3G wireless modem USB-based interface	SRX100, SRX110, and SRX210 only	No	No	No
3G wireless modem interface using the CX111 external wireless bridge	Yes	Yes	No	Yes
ADSL interface	SRX110, SRX210, SRX220, and SRX240 only	SRX550 only	No	Yes
Channelized E1/T1 interface	No	No	No	Yes
Channelized ISDN PRI interface	No	No	No	Yes
DOCSIS Mini-PIM interface	SRX210, SRX220, and SRX240 only	SRX550 only	No	No
Fractional and clear channel DS3/E3 interface	No	Yes	No	Yes
Ethernet interface	Yes	Yes	Yes	Yes
Fast Ethernet interface	SRX100, SRX110, and SRX210 only	NO	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

Table 23: Physical and Virtual Interface Support *(continued)*

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
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	Yes	No	Yes
Symmetric high-speed digital subscriber line (G.SHDSL) interface	SRX210, SRX220, and SRX240 only	SRX550 only	No	Yes
USB modem physical interface	Yes	No	No	Yes
VDSL interface	SRX110, SRX210, SRX220, and SRX240	SRX550 only	No	No
VDSL over POTS	SRX110-VA, SRX210, SRX220, and SRX240 only	SRX550 only	No	No
VDSL over ISDN-BRI	SRX110-VB only	No	No	No

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

Table 24: Services Support

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Aggregated Ethernet interface	Yes	Yes	Yes	Yes
GRE interface	Yes	Yes	Yes	Yes

Table 24: Services Support *(continued)*

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
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-supplicant support	Yes	Yes	No	Yes
Interleaving using MLFR	Yes	Yes	No	Yes
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	Yes	Yes	Yes
Internally generated Protocol Independent Multicast encapsulation interface	Yes	Yes	Yes	Yes
Link fragmentation and interleaving interface	Yes	Yes	No	No

Table 24: Services Support *(continued)*

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Link services interface	Yes	Yes	No	Yes
Loopback interface	Yes	Yes	Yes	Yes
Management interface	Yes	Yes	Yes	Yes
PPP interface	Yes	Yes	No	Yes
PPPoE-based radio-to-router protocol	Yes	Yes	Yes	Yes
PPPoE interface	Yes	Yes	No	No
Promiscuous mode on interfaces	No	No	Yes	No
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 25 on page 30 lists IDP features that are supported on SRX Series and J Series devices.

Table 25: IDP Support

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 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

Table 25: IDP Support *(continued)*

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Application identification See "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	No	No	Yes	No
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	SRX210, SRX220, 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
IDP signature database	Yes	Yes	Yes	Yes
IDP SSL inspection	No	No	Yes	No
IPS rule base	Yes	Yes	Yes	Yes

Table 25: IDP Support *(continued)*

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Jumbo frames	Yes	Yes	Yes (9192 bytes)	Yes (9010 bytes)
Nested application identification (Extended application identification)	Yes	Yes	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 Monitoring

SRX100, SRX210, SRX220, SRX240, and SRX650 Services Gateways support IP monitoring. This feature monitors IP addresses on standalone SRX Series Services Gateways. The feature enables a device to track the reachability of a particular IP address.

Table 26 on page 32 shows the SRX Series devices that support IP monitoring.

Table 26: IP Monitoring Support

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
IP monitoring with route failover (for standalone devices and redundant Ethernet interfaces)	Yes	Yes	No	No
IP monitoring with interface failover (for standalone devices)	Yes	Yes	No	No

Related Documentation

- *Junos OS Monitoring and Troubleshooting Guide for Security Devices*

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 27 on page 33 lists IPsec features that are supported on SRX Series and J Series devices.

Table 27: IPsec Support

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
AH protocol	Yes	Yes	Yes	Yes
Alarms and auditing	Yes	Yes	No	No
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
IKEv2	Yes	Yes	Yes	No
Manual key management	Yes	Yes	Yes	Yes

Table 27: IPsec Support *(continued)*

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
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 28 on page 34 lists the SRX Series and J Series device features that support IPv6.

Table 28: IPv6 Support

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Chassis cluster				
Active-active	SRX100, SRX210, SRX220, and SRX240 only	Yes	Yes	Yes

Table 28: IPv6 Support *(continued)*

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Active-passive	SRX100, SRX210, SRX220, and SRX240 only	Yes	Yes	Yes
Multicast flow	SRX100, SRX210, SRX220, and SRX240 only	Yes	Yes	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)	Yes	Yes	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)	No	No	Yes	No
Security policy (user role firewall)	No	No	No	No
Zones	Yes	Yes	Yes	Yes
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

Table 28: IPv6 Support *(continued)*

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
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
IPv6 IDP/AppSecure				
Application DDoS (AppDoS)	No	No	No	No
Application Firewall (AppFW)	Yes	Yes	Yes	No
Application QoS (AppQoS)	No	No	Yes	No
Application Tracking (AppTrack)	No	No	No	No
IDP	No	No	Yes	No
Logical systems				
Admin operations (Telnet, SSH, HTTPS, and so on.)	No	No	Yes	No
Chassis clusters	No	No	Yes	No
Firewall authentication	No	No	Yes	No
Flows	No	No	Yes	No

Table 28: IPv6 Support *(continued)*

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Interfaces	No	No	Yes	No
IPv6 dual-stack lite (DS-Lite)	No	No	Yes	No
NAT (except interface NAT)	No	No	Yes	No
Routing (BGP only)	No	No	Yes	No
Screen options	No	No	Yes	No
Zones and security policies	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

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 29 on page 38 lists the IPv6 IPsec features that are supported on the SRX Series and J Series devices.

Table 29: IPv6 IP Security Support

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
4in4 and 6in6 policy-based site-to-site VPN, AutoKey IKEv1	Yes	Yes	No	Yes
4in4 and 6in6 policy-based site-to-site VPN, manual key	Yes	Yes	No	Yes
4in4 and 6in6 route-based site-to-site VPN, AutoKey IKEv1	Yes	Yes	No	Yes
4in4 and 6in6 route-based site-to-site VPN, manual key	Yes	Yes	No	Yes
IKEv1 authentication, preshared key	Yes	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 30 on page 38 describes the Junos OS features that require licenses.

Table 30: Junos OS Feature Licenses

Junos OS License Requirements	Device										
Feature	J Series	SRX 100	SRX 110	SRX 210	SRX 220	SRX 240	SRX 550	SRX 650	SRX 1000 line	SRX 3000 line	SRX 5000 line
Access Manager		X	X	X	X	X	X	X			
BGP Route Reflectors	X							X			
Dynamic VPN		X	X	X	X	X	X	X			

Table 30: Junos OS Feature Licenses *(continued)*

Junos OS License Requirements	Device									
Feature	J Series	SRX 100	SRX 110	SRX 210	SRX 220	SRX 240	SRX 550	SRX 650	SRX 1000 line	SRX 3000 line	SRX 5000 line
IDP Signature Update	X	X *	X	X *	X *	X *	X	X	X	X	X
Application Signature Update (Application Identification)	X	X	X	X	X	X	X	X	X	X	X
Juniper-Kaspersky Anti-Virus	X	X	X	X	X	X	X	X			
Juniper-Sophos Anti-Spam	X	X	X	X	X	X	X	X			
Juniper-Websense Integrated Web Filtering	X	X	X	X	X	X	X	X			
SRX100 Memory Upgrade		X									
UTM	X	X*	X	X *	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 31 on page 40 lists the Layer 2 features that are supported on SRX Series and J Series devices.

Table 31: Layer 2 Mode Support

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
802.1x port-based network authentication	Yes	Yes	No	Yes
Flexible Ethernet services	Yes	Yes	No	Yes
Generic VLAN registration protocol	Yes	Yes	No	Yes
IGMP snooping	Yes	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 NOTE: MSTP is not supported on SRX210 or SRX220.	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*

Log File Formats

Junos OS generates separate log messages to record events that occur on the system's control and data planes. The control plane logs (called system logs) include events that occur on the routing platform. The data plane logs (called security logs) primarily include security events that the system has handled directly inside the data plane.

Table 32 on page 41 lists the system and security log file formats supported on SRX Series and J Series devices.

Table 32: Security Log File Formats

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
System (Control Plane) Log File Formats				
Binary format (binary)	No	No	No	No
Structured syslog (sd-syslog)	Yes	Yes	Yes	Yes
Syslog (syslog)	Yes	Yes	Yes	Yes
WebTrends Enhanced Log Format (welf)	No	No	No	No
Security (Data Plane) Log File Formats				
Binary format (binary)	Yes	Yes	Yes	No
Structured syslog (sd-syslog)	Yes	Yes	Yes	Yes
Syslog (syslog)	Yes	Yes	Yes	Yes
WebTrends Enhanced Log Format (welf)	Yes	Yes	Yes	Yes

Related Documentation

- *Junos OS Security Configuration Guide*

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 33 on page 42 lists features of logical systems that are supported on SRX Series devices.

Table 33: Logical Systems Support

Feature	SRX100 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Administration	No	No	Yes	No
Application identification	No	No	Yes	No
Application tracking	No	No	Yes	No
Application firewall	No	No	Yes	No
Chassis cluster	No	No	Yes	No
CPU utilization	No	No	Yes	No
Data path debugging	No	No	Yes	No
Firewall authentication	No	No	Yes	No
Interfaces	No	No	Yes	No
Intrusion detection and prevention	No	No	Yes	No
IPv6 addresses for:				
• Admin operations (Telnet, SSH, HTTPS, and so on.)	No	No	Yes	No
• Chassis clusters	No	No	Yes	No
• Firewall authentication	No	No	Yes	No
• Flows	No	No	Yes	No
• Interfaces	No	No	Yes	No
• IPv6 dual-stack lite (DS-Lite)	No	No	Yes	No
• NAT (except for interface NAT)	No	No	Yes	No
• Routing (BGP only)	No	No	Yes	No

Table 33: Logical Systems Support *(continued)*

Feature	SRX100 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
• Screen options	No	No	Yes	No
• Zones and security policies	No	No	Yes	No
J-Web logical system configuration and monitoring	No	No	Yes	No
Licensing	No	No	Yes	No
Multicast	No	No	Yes	No
Network address translation	No	No	Yes	No
Routing, dynamic and static	No	No	Yes	No
Screen options	No	No	Yes	No
Security logs (include logical system names)	No	No	Yes	No
Security policies	No	No	Yes	No
Security profiles	No	No	Yes	No
Sessions	No	No	Yes	No
VPN tunnel interface	No	No	Yes	No
Zones	No	No	Yes	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 34 on page 44 lists the management features that are supported on SRX Series and J Series devices.

Table 34: Management Feature Support

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 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 35 on page 44 lists the MPLS features that are supported on SRX Series and J Series devices.

Table 35: MPLS Feature Support

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 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

Table 35: MPLS Feature Support *(continued)*

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
LDP	Yes	Yes	No	Yes
MPLS VPNs with VRF tables on provider edge routers	Yes	Yes	No	Yes
Multicast VPNs	Yes	Yes	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 36 on page 46 lists the multicast features that are supported on SRX Series and J Series devices.

Table 36: Multicast Support

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 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 37 on page 47 lists the multicast VPN features that are supported on J Series devices.

Table 37: Multicast VPN Support

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Basic multicast features in C-instance	Yes	Yes	No	Yes
Multicast VPN membership discovery with BGP	Yes	Yes	No	Yes
P2MP LSP support	Yes	Yes	No	Yes
P2MP OAM - P2MP LSP ping	Yes	Yes	No	Yes
Reliable multicast VPN routing information exchange	Yes	Yes	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 38 on page 47 lists NAT features that are supported on SRX Series and J Series devices.

Table 38: NAT Support

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 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

Table 38: NAT Support *(continued)*

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Interface source NAT pool port	Yes	Yes	Yes	Yes
NAT address pool utilization threshold status	Yes	Yes	Yes	Yes
NAT traversal (NAT-T) for site-to-site IPsec VPNs (IPv4)	Yes	Yes	Yes	Yes
Persistent NAT	Yes	Yes	Yes	Yes
Persistent NAT binding for wildcard ports	Yes	Yes	Yes	Yes
Persistent NAT hairpinning	Yes	Yes	Yes	Yes
Pool translation	Yes	Yes	Yes	Yes
Proxy ARP (IPv4)	Yes	Yes	Yes	Yes
Proxy NDP (IPv6)	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
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 39 on page 49 lists the network operations features that are supported on SRX Series and J Series devices.

Table 39: Network Operations and Troubleshooting Support

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 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 40 on page 50 lists the packet capture support on SRX Series and J Series devices.

Table 40: Packet Capture Support

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 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 41 on page 50 lists the PoE support on SRX Series and J Series devices.

Table 41: PoE Support

Feature	SRX100 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
IEEE 802.3 AF standard	SRX210 (PoE), SRX220 (PoE), and SRX240 (PoE)	Yes	No	No
IEEE 802.3 AT standard	SRX210 (PoE), SRX220 (PoE), and SRX240 (PoE)	Yes	No	No
IEEE legacy (pre-standards)	SRX210 (PoE), SRX220 (PoE), and SRX240 (PoE)	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 42 on page 51 lists the PKI features that are supported on SRX Series and J Series devices.

Table 42: PKI Support

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 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
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 CRLretrieval 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 43 on page 52 lists the RPM probe support on SRX Series and J Series devices.

Table 43: RPM Probe Support

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 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 44 on page 52 lists the remote device access support on SRX Series and J Series devices.

Table 44: Remote Device Access Support

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Reverse Telnet	No	No	No	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 45 on page 53 lists the routing features that are supported on SRX Series and J Series devices.

Table 45: Routing Support

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
BGP	Yes	Yes	Yes	Yes
BGP extensions for IPv6	Yes	Yes	Yes	Yes
Compressed Real-Time Transport Protocol (CRTP)	Yes	Yes	No	Yes
ECMP flow-based forwarding	Yes	Yes	Yes	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

Table 45: Routing Support *(continued)*

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
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 46 on page 54 lists the secure web access features that are supported on SRX Series and J Series devices.

Table 46: Secure Web Access Support

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 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. Global policies allow you to regulate traffic with addresses and applications, regardless of their security zones.

Table 47 on page 55 lists the security policy features that are supported on SRX Series and J Series devices.

Table 47: Security Policy Support

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Address books/Address sets	Yes	Yes	Yes	Yes
Custom policy applications	Yes	Yes	Yes	Yes
Global Policy	Yes	Yes	Yes	Yes
Policy application timeouts	Yes	Yes	Yes	Yes
Policy applications and application sets	Yes	Yes	Yes	Yes
Policy hit-count tracking	Yes	Yes	Yes	Yes
Schedulers	Yes	Yes	Yes	Yes
Security policies for self-traffic	Yes	Yes	Yes	Yes
SSL Proxy	No	No	Yes	No
User role firewall	Yes	Yes	Yes	No
Common predefined 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 48 on page 56 lists the zones supported on SRX Series and J Series devices.

Table 48: Zones Support

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 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*

Services Offloading

Services offloading is a mechanism for processing fast-path packets in the network processor instead of in the Services Processing Unit (SPU). This method reduces the long packet processing latency that arises when packets are forwarded from network processors to SPUs for processing and back to I/O cards (IOCs) for transmission.

Services offloading considerably reduces packet processing latency by 500-600 percent.

When the first packet arrives at the interface, the network processor forwards it to the SPU for processing. If the SPU verifies that the traffic is qualified for services offloading, a services-offload session is created on the network processor. If the traffic does not qualify for services offloading, a normal session is created on the network processor. If a services-offload session is created, subsequent fast-path packets are processed in the network processor itself.

Table 49 on page 57 lists the services offloading features supported on SRX Series and J Series devices.

Table 49: Services Offloading Support

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Services Offloading	No	No	Yes	No

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 50 on page 57 lists the session logging features that are supported on SRX Series and J Series devices.

Table 50: Session Logging Support

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Accelerating security and traffic logging	Yes	Yes	Yes	Yes
Aggressive session aging	Yes	Yes	Yes	No
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 51 on page 58 lists the SRX Series and J Series devices that support SMTP.

Table 51: SMTP Support

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 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 52 on page 58 lists the SNMP support on SRX Series and J Series devices.

Table 52: SNMP Support

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
SNMP v1, v2, v3	Yes	Yes	Yes	Yes

Related Documentation

- Juniper Networks Enterprise-Specific SNMP Traps

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 53 on page 59 lists the stateless firewall filters support on SRX Series and J Series devices.

Table 53: Stateless Firewall Filters Support

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Stateless firewall filters (ACLs)	Yes	Yes	Yes	Yes
Stateless firewall filters (Simple Filter)	No	No	Yes	No

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 54 on page 59 lists the system log files features that are supported on SRX Series and J Series devices.

Table 54: System Log Files Support

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 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

Table 54: System Log Files Support *(continued)*

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Multiple system log servers (control-plane logs)	Yes	Yes	Yes	Yes
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 55 on page 60 lists the transparent mode features that are supported on SRX Series devices.

Table 55: Transparent Mode Support

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Application DoS (AppDDoS)	No	No	No	No
Application Firewall (AppFW)	No	No	Yes	No

Table 55: Transparent Mode Support *(continued)*

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Application QoS (AppQoS)	No	No	Yes	No
Application Tracking (AppTrack)	No	No	Yes*	No
Bridge domain and transparent mode	Yes	Yes	Yes	No
Chassis clusters (active/backup and active/active)	SRX100, SRX210, SRX220, and SRX240 only	Yes	Yes	No
Class of service	Yes	Yes	Yes	No
User role firewall	No	No	Yes	No

*Interval update not supported.

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 56 on page 61 lists the UTM features that are supported on SRX Series and J Series devices.

Table 56: UTM Support

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Antispam	Yes	Yes	No	Yes
Antivirus Express	SRX210, SRX220, and SRX240 only.	Yes	No	Yes

Table 56: UTM Support *(continued)*

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Antivirus Full	Yes	Yes	No	Yes
Antivirus Sophos	Yes	Yes	No	No
Chassis cluster (active/active chassis cluster with the Packet Forwarding Engine active on both the cluster nodes [the Packet Forwarding Engine and the Routing Engine active in the same node])	SRX100, SRX210, SRX220, and SRX240 only	Yes	No	No
Content filtering	Yes	Yes	No	Yes
Enhanced Web filtering	Yes	Yes	No	No
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 57 on page 63 lists the upgrading and rebooting features that are supported on SRX Series and J Series devices.

Table 57: Upgrading and Rebooting Support

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Autorecovery	Yes	Yes	No	No
Boot device configuration	Yes	Yes	Yes	Yes
Boot device recovery	Yes	Yes	Yes	Yes
Chassis components control	Yes	Yes	Yes	Yes
Chassis restart	Yes	Yes	Yes	Yes
Download manager	Yes	Yes	No	No
Dual-root partitioning	Yes	Yes	No	Yes
In-band cluster upgrade	Yes	Yes	No	No
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 58 on page 64 lists the USB modem support for SRX Series devices.

Table 58: USB Modem Support

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 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 59 on page 64 lists the user interface features that are supported on SRX Series and J Series devices.

Table 59: User Interfaces Support

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 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 60 on page 65 lists the VoIP with Avaya features that are supported only on J Series devices.

Table 60: VoIP with Avaya Support

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Avaya Communication Manager	No	No	No	Yes
Avaya VoIP Modules: • 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	No	No	No	Yes
Dynamic Call Admission Control	No	No	No	Yes
Media Gateway Controller	No	No	No	Yes
VoIP interfaces: • Analog telephone or trunk port • E1 port • ISDN BRI telephone or trunk port • T1 port	No	No	No	Yes

Related Documentation

- *Junos OS Interfaces Configuration Guide for Security Devices*

VPLS

Virtual private LAN service (VPLS) is an Ethernet-based Point-to-Multipoint Layer 2 VPN. It allows you to connect geographically dispersed Ethernet LAN sites to each other across an MPLS backbone. For customers who implement VPLS, all sites appear to be in the same Ethernet LAN even though traffic travels across the service provider's network.

Table 61 on page 66 lists the VPLS features that are supported on SRX Series and J Series devices.

Table 61: VPLS Feature Support

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Filtering and Policing (Packet-Based)	Yes	Yes	No	Yes

Related Documentation

- *Junos OS MPLS 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 62 on page 66 lists the WLAN support on SRX Series and J Series devices.

Table 62: Wireless LAN Support

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Wireless LAN	Yes	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