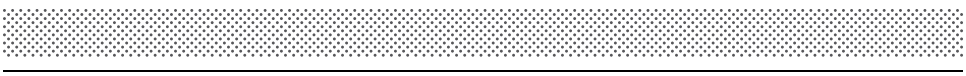
JUNIPER NETWORKS

Junos® OS

Feature Support Reference for Junosphere VSRX

Release
2.7



Published: 2013-01-16

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

Junos OS Feature Support Reference for Junosphere VSRX
Release 2.7

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.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at http://www.juniper.net/support/eula.html. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About This Guide

This preface provides the following guidelines for using the *Junos OS Feature Support Reference for Junosphere VSRX*:

Junosphere VSRX Documentation and Release Notes

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 Junosphere VSRX running Junos OS.

Document Conventions

Table 1 on page vi 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 vi 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 or emphasizes 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; 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 Junosphere VSRX

CHAPTER 1

Overview

Feature Support Overview

Junosphere VSRX is a virtual security appliance that provides security and networking services at the perimeter or edge in virtualized private or public cloud environments. Junosphere VSRX runs as a virtual machine (VM) on a standard x86 server.

Junosphere VSRX enables advanced security and routing at the network edge in a multitenant virtualized environment. Junosphere VSRX is built on Junos OS and delivers the same core networking and security features available on SRX Series devices for the branch.

Some of the key benefits of Junosphere VSRX in virtualized private or public cloud multitenant environments include:

- Stateful firewall protection at the tenant edge
- Faster deployment of virtual firewalls
- Full routing and networking capabilities
- Complementary with the Juniper Networks vGW Virtual Gateway for inter-VM security
- Centralized and local management

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 changes made to an address set automatically applies 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 Junosphere VSRX.

Table 3: Address Books and Address Sets Support

Feature	Junosphere VSRX
Address books	Yes
Address sets	Yes
Global address objects or sets	Yes
Nested address groups	Yes

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 Junosphere VSRX.

Table 4: Administrator Authentication Support

Feature	Junosphere VSRX
Local authentication	Yes
RADIUS	Yes
TACACS+	Yes

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 Junosphere VSRX.

Table 5: Alarm Support

Feature	Junosphere VSRX
Chassis alarms	Yes
Interface alarms	Yes
System alarms	Yes

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 Junosphere VSRX 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 Junosphere VSRX. Also, ALGs modify the embedded IP addresses as required.

Table 6 on page 9 lists the ALG features that are supported on Junosphere VSRX.

Table 6: ALG Support

Feature	Junosphere VSRX
DNS ALG	Yes
DNS doctoring support	Yes
DNS, FTP, RTSP, and TFTP ALGs (Layer 2) with chassis clustering	No
DSCP marking for SIP, H.323, MGCP, and SCCP ALGs	Yes
FTP	Yes
H.323	Yes
Avaya H.323	Yes
IKE	Yes
MGCP	Yes
PPTP	Yes
RSH	Yes
RTSP	Yes
SCCP	Yes
SIP	Yes
SIP ALG–NEC	Yes
SQL	Yes
MS RPC	Yes
SUN RPC	Yes
TALK	Yes
TFTP	Yes

Attack Detection and Prevention

Attack detection and prevention 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, network resource, clients or servers.

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 7 on page 10 lists the attack detection and prevention features that are supported on Junosphere VSRX.

Table 7: Attack Detection and Prevention Support

Feature	Junosphere VSRX
Bad IP option	Yes
Block fragment traffic	Yes
FIN flag without ACK flag set protection	Yes
ICMP flood protection	Yes
ICMP fragment protection	Yes
IP address spoof	Yes
IP address sweep	Yes
IP record route option	Yes
IP security option	Yes
IP stream option	Yes
IP strict source route option	Yes
IP timestamp option	Yes
Land attack protection	Yes
Large size ICMP packet protection	Yes
Loose source route option	Yes

Table 7: Attack Detection and Prevention Support *(continued)*

Feature	Junosphere VSRX
Ping of death attack protection	Yes
Port scan	Yes
Source IP-based session limit	Yes
SYN-ACK-ACK proxy protection	Yes
SYN and FIN flags set protection	Yes
SYN flood protection	Yes
SYN fragment protection	Yes
TCP address sweep	Yes
TCP packet without flag set protection	Yes
Teardrop attack protection	Yes
UDP address sweep	Yes
UDP flood protection	Yes
Unknown IP protocol protection	Yes
Whitelist for SYN flood screens	Yes
WinNuke attack protection	Yes

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 disk. 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 disk. The autoinstallation feature enables you to deploy multiple devices from a central location in the network.

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 8 on page 12 lists the CoS features that are supported on Junosphere VSRX.

Table 8: CoS Support

Feature	Junosphere VSRX
Classifiers	Yes
Code-point aliases	Yes
Egress interface shaping	Yes
Forwarding classes	Yes
High-priority queue on Services Processing Card	Yes
Ingress interface policer	Yes
Schedulers	Yes
Simple filters	Yes
Transmission queues	Yes
Tunnels NOTE: GRE and IP-IP tunnels only.	Yes
Virtual channels	Yes

Diagnostics Tools

Junosphere VSRX 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 9 on page 13 lists the features of the diagnostics tools that are supported on Junosphere VSRX.

Table 9: Diagnostics Tools Support

Feature	Junosphere VSRX
CLI terminal	Yes
J-Flow versions 5 and version 8	Yes
J-Flow version 9	Yes
Ping host	Yes
Ping MPLS	Yes
Traceroute	Yes
Ping Ethernet (CFM)	Yes
Traceroute Ethernet (CFM)	Yes

DNS Proxy

A domain name service (DNS) proxy allows clients to use a device as a DNS proxy server. Use of a DNS proxy improves domain lookup performance by caching previous lookups. A typical DNS proxy processes DNS queries by issuing a new DNS resolution query to each name server that it has detected until the hostname is resolved.

Table 10 on page 13 lists the DNS proxy features that are supported on Junosphere VSRX.

Table 10: DNS Proxy Support

Feature	Junosphere VSRX
DNS proxy cache	Yes
DNS proxy with split DNS	Yes
Dynamic DNS	Yes

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 11 on page 14 lists the DHCP features that are supported on Junosphere VSRX.

Table 11: DHCP Support

Feature	Junosphere VSRX
DHCPv6 client	No
DHCPv4 client	Yes
DHCPv6 relay agent	No
DHCPv4 relay agent	Yes
DHCPv6 server	Yes
DHCPv4 server	Yes
DHCP server address pools	Yes
DHCP server static mapping	Yes

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.

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.

Junosphere VSRX provides Ethernet Link Aggregation support in routing mode only.

Table 12 on page 15 lists the Ethernet link aggregation features that are supported on Junosphere VSRX.

Table 12: Ethernet Link Aggregation Support

Feature	Junosphere VSRX
Routing mode	
LACP in chassis cluster pair	No
LACP in standalone device	Yes
Layer 3 LAG on routed ports	Yes
Static LAG in chassis cluster mode	No
Static LAG in standalone mode	Yes

Ethernet Link Fault Management

The Ethernet interfaces on the Junosphere VSRX support the IEEE 802.3ah standard for Operation, Administration, and Maintenance (OAM). The standard defines OAM link fault management (LFM).

Junosphere VSRX provides Ethernet Link Fault Management support in routing mode only.

Table 13 on page 15 lists the LFM features that are supported on Junosphere VSRX in routing mode.

Table 13: Ethernet Link Fault Management Support in Routing Mode

Feature	Junosphere VSRX
Interfaces supported:	
LACP in chassis cluster pair	No
LACP in standalone mode	Yes
Static LAG in chassis cluster mode	No
Static LAG in standalone mode	Yes
Physical interface (encapsulations)	
ethernet-ccc	No
extended-vlan-ccc	No
ethernet-tcc	No

Table 13: Ethernet Link Fault Management Support in Routing Mode *(continued)*

Feature	Junosphere VSRX
extended-vlan-tcc	No
Interface family	
inet	Yes
mpls	Yes
ccc	No
tcc	No
iso	Yes
ethernet-switching	No
inet6	Yes
Aggregated Ethernet interface:	
Static LAG	Yes
LACP enabled LAG	Yes
Interface family	
ethernet-switching	No
inet	Yes
inet6	Yes
iso	Yes
mpls	Yes

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 14 on page 17 lists the file management features that are supported on Junosphere VSRX.

Table 14: File Management Support

Feature	Junosphere VSRX
Clean up unnecessary files	Yes
Delete backup software image	Yes
Delete individual files	Yes
Download system files	Yes
Encrypt/decrypt configuration files	Yes
Manage account files	Yes
Rescue	Yes
System snapshot	Yes
System zeroize	Yes
Monitor start	Yes
Archive files	Yes
Calculate checksum	Yes
Compare files	Yes
Rename files	Yes

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 15 on page 18 lists firewall authentication features that are supported on Junosphere VSRX.

Table 15: Firewall Authentication Support

Feature	Junosphere VSRX
Firewall authentication on Layer 2 transparent authentication	No
LDAP authentication server	Yes
Local authentication server	Yes
Pass-through authentication	Yes
RADIUS authentication server	Yes
SecurID authentication server	Yes
Web authentication	Yes

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 16 on page 19 lists the flow-based and packet-based features that are supported on Junosphere VSRX.

Table 16: Flow-Based and Packet-Based Processing Support

Feature	Junosphere VSRX
Alarms and auditing	Yes
End-to-end packet debugging	No
Flow-based processing	Yes
Network processor bundling	No
Packet-based processing	Yes
Selective stateless packet-based services	Yes

Interfaces

All Juniper Networks devices use network interfaces to connect to other devices. 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 17 on page 19 lists the features of the physical and virtual interfaces that are supported on Junosphere VSRX.

Table 17: Physical and Virtual Interface Support

Feature	Junosphere VSRX
Ethernet interface	Yes
Gigabit Ethernet interface	Yes

Table 18 on page 19 lists the features of the services that are supported on Junosphere VSRX.

Table 18: Services Support

Feature	Junosphere VSRX
Aggregated Ethernet interface	Yes
GRE interface	Yes
IEEE 802.1X dynamic VLAN assignment	Yes

Table 18: Services Support *(continued)*

Feature	Junosphere VSRX
IEEE 802.1X MAC bypass	Yes
IEEE 802.1X port-based authentication control with multisupplicant support	Yes
Interleaving using MLFR	No
Internally configured interface used by the system as a control path between the WXC Integrated Services Module and the Routing Engine	No
Internally generated GRE interface (gr-0/0/0)	Yes
Internally generated IP-over-IP interface (ip-0/0/0)	Yes
Internally generated link services interface	Yes
Internally generated Protocol Independent Multicast de-encapsulation interface	Yes
Internally generated Protocol Independent Multicast encapsulation interface	Yes
Link fragmentation and interleaving interface	Yes
Link services interface	Yes
Loopback interface	Yes
Management interface	Yes
PPP interface	No
PPPoE-based radio-to-router protocol	No
PPPoE interface	No
Promiscuous mode on interfaces	Yes NOTE: Promiscuous mode needs to be enabled on hypervisor.
Secure tunnel interface	Yes

IP Monitoring

The IP monitoring feature monitors IP addresses and enables the device to track the reachability of a particular IP address. Existing real-time performance monitoring (RPM) probes are sent to an IP address to check for reachability. Each probed target is monitored over the course of a test. During a test, probes are generated and responses collected at a rate defined by the probe interval, which is the number of seconds between probes.

Table 19 on page 21 lists the IP monitoring features that are supported on Junosphere VSRX.

Table 19: IP Monitoring Support

Feature	Junosphere VSRX
IP monitoring with route failover (for standalone devices and redundant Ethernet interfaces)	Yes
IP monitoring with interface failover (for standalone devices)	Yes

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 that 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.

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).

The dynamic VPN feature simplifies remote access by enabling users to establish IP Security (IPsec) VPN tunnels without having to manually configure VPN settings on their Windows 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 20 on page 22 lists IPsec features that are supported on Junosphere VSRX.

Table 20: IPsec Support

Feature	Junosphere VSRX
Acadia - Clientless VPN	Yes
AH protocol	Yes
Alarms and auditing	Yes
Antireplay (packet replay attack prevention)	Yes
Authentication	Yes
Authentication Header (AH)	Yes
Autokey management	Yes
Automated certificate enrollment using SCEP	Yes
Automatic generation of self-signed certificates	Yes
Bridge domain and transparent mode	No
Certificate - Configure local certificate sent to peer	Yes
Certificate - Configure requested CA of peer certificate	Yes
Certificate - Encoding: PKCS7, X509, PEM, DERs	Yes
Certificate - RSA signature	Yes
Chassis clusters (active/backup and active/active)	No
Class of service	Yes
CRL update at user-specified interval	Yes
Config Mode (draft-dukes-ike-mode-cfg-03)	Yes
Dead Peer Detection (DPD)	Yes
Diffie-Hellman (PFS) Group 1	Yes
Diffie-Hellman (PFS) Group 2	Yes
Diffie-Hellman (PFS) Group 5	Yes
Diffie-Hellman Group 1	Yes

Table 20: IPsec Support *(continued)*

Feature	Junosphere VSRX
Diffie-Hellman Group 2	Yes
Diffie-Hellman Group 5	Yes
Digital signature generation	Yes
Dynamic IP address	Yes
Dynamic IPsec VPNs	Yes
Encapsulating Security Payload (ESP) protocol	Yes
Encryption Algorithms 3DES	Yes
Encryption Algorithms AES 128, 192, and 256	Yes
Encryption Algorithms DES	Yes
Encryption Algorithms NULL (authentication only)	Yes
Entrust, Microsoft, and Verisign certificate authorities (CAs)	Yes
External Extended Authentication (Xauth) to a RADIUS server for remote access connections	Yes
Group Encrypted Transport (GET VPN)	No
Group VPN with dynamic policies	No
Hard lifetime limit	Yes
Hardware IPSec (bulk crypto) Cavium/RMI	No
Hash Algorithms MD5	Yes
Hash Algorithms SHA-1	Yes
Hash Algorithms SHA-2 (SHA-256)	Yes
Hub & Spoke VPN	Yes
Idle timers for IKE	Yes
Improvements in VPN Debug Capabilities	Yes
Initial Contact	Yes

Table 20: IPsec Support *(continued)*

Feature	Junosphere VSRX
Invalid SPI response	Yes
IKE Diffie-Hellman Group 14 support	Yes
IKE Phase 1	Yes
IKE Phase 1 lifetime	Yes
IKE Phase 2	Yes
IKE Phase 2 lifesize	Yes
IKE and IPSEC pre-define proposal sets to work with Dynamic VPN client	Yes
IPSec tunnel termination in routing-instances	Yes
IKE support	Yes
IKEv1	Yes
IKEv1 authentication, preshared key	Yes
IKEv2	Yes
Local IP address Management - VPN XAuth support	Yes
Local IP address Management Support for DVPN	Yes
Manual installation of DER-encoded and PEM-encoded CRLs	Yes
Manual key management	Yes
Manual proxy-ID (Phase 2 ID) configuration	Yes
NHTB - Next Hop Tunnel Binding	Yes
New IPSec Phase 2 Authentication Algorithm	Yes
Online CRLretrieval through LDAP and HTTP	Yes
Package dynamic VPN client	Yes
Policy-based VPN	Yes
Preshared key (PSK)	Yes

Table 20: IPsec Support *(continued)*

Feature	Junosphere VSRX
Prioritization of IKE packet processing	Yes
Reconnect to dead IKE peer	Yes
Remote Access	Yes
Remote Access user IKE peer	Yes
Remote Access user-group IKE peer - group IKE ID	Yes
Route-based VPN	Yes
SHA-2 IPSec support	Yes
Soft lifetime	Yes
Static IP address	Yes
Suites: Standard, Compatible, Basic, and custom-created	Yes
Support for NHTB when the st0.x interface is bound to a routing instance	Yes
Support for Remote Access peers with shared IKE identity + mandatory XAuth	Yes
Support group IKE IDs for Dynamic VPN configuration	Yes
TOS/DSCP honoring/coloring (inner/outer)	Yes
Tunnel Mode with clear/copy/set Don't Fragment bit	Yes
UAC Layer 3 enforcement	Yes
Virtual router support for route-based VPNs	Yes
VPN monitoring (proprietary)	Yes
X.509 encoding for IKE	Yes
XAuth (draft-beaulieu-ike-xauth-03)	Yes

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—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 21 on page 26 lists the IPv6 features that are supported on Junosphere VSRX.

Table 21: IPv6 Support

Feature	Junosphere VSRX
Flow-based forwarding and security features	
Advanced flow	Yes
DS-Lite concentrator (aka AFTR)	No
DS-Lite initiator (aka B4)	No
Firewall filters	Yes
Forwarding option: flow mode	Yes
Multicast flow	Yes
Screens	Yes
Security policy (firewall)	Yes
Security policy (IDP)	No
Security policy (user role firewall)	No
Zones	Yes
IPv6 ALG support for FTP Routing, NAT, NAT-PT support	Yes

Table 21: IPv6 Support *(continued)*

Feature	Junosphere VSRX
IPv6 ALG support for ICMP Routing, NAT, NAT-PT support	Yes
IPv6 NAT NAT-PT, NAT support	Yes
IPv6 NAT64	Yes
IPv6–related protocols BFD, BGP, ECMPv6, ICMPv6, ND, OSPFv3, RIPng	Yes
IPv6 ALG support for TFTP	Yes
System services DHCPv6, DNS, FTP, HTTP, ping, SNMP, SSH, syslog, Telnet, traceroute	Yes
Packet-based forwarding and security features	
Class of service	Yes
Firewall filters	Yes
Forwarding option: packet mode	Yes

IPv6 IP Security

IPv6 IP Security (IPsec) is the implementation of the IPsec suite of protocols in IPv6 networks. IPsec provides interoperable, high quality, and cryptographically based security services for traffic at the IP layer. In IPv6, IPsec enhances the original IP protocol by providing authenticity, integrity, confidentiality, and access control to each IP packet through the use of two protocols: authentication header (AH) and Encapsulating Security Payload (ESP).

Table 22 on page 27 lists the IPv6 IPsec features that are supported on Junosphere VSRX.

Table 22: IPv6 IP Security Support

Feature	Junosphere VSRX
4in4 and 6in6 policy-based site-to-site VPN, AutoKey IKEv1	Yes
4in4 and 6in6 policy-based site-to-site VPN, manual key	Yes
4in4 and 6in6 route-based site-to-site VPN, AutoKey IKEv1	Yes
4in4 and 6in6 route-based site-to-site VPN, manual key	Yes

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 23 on page 28 lists the system and security log file formats supported on Junosphere VSRX.

Table 23: Security Log File Formats

Feature	Junosphere VSRX
System (Control Plane) Log File Formats	
Binary format (binary)	No
Structured syslog (sd-syslog)	Yes
Syslog (syslog)	Yes
WebTrends Enhanced Log Format (welf)	No
Security (Data Plane) Log File Formats	
Binary format (binary)	Yes
Structured syslog (sd-syslog)	Yes
Syslog (syslog)	Yes
WebTrends Enhanced Log Format (welf)	Yes

MPLS

MPLS provides a framework for controlling traffic patterns across a network. The MPLS framework allows Junosphere VSRX 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 24 on page 29 lists the MPLS features that are supported on Junosphere VSRX.

Table 24: MPLS Feature Support

Feature	Junosphere VSRX
CCC and TCC	Yes
CLNS	Yes
Interprovider and carrier-of-carriers VPNs	Yes
Layer 2 VPNs for Ethernet connections	Yes
Layer 3 MPLS VPNs	Yes
LDP	Yes
MPLS VPNs with VRF tables on provider edge routers	Yes
Multicast VPNs	Yes
OSPF and IS-IS traffic engineering extensions	Yes
P2MP LSPs	Yes
RSVP	Yes
Secondary and standby LSPs	Yes
Standards-based fast reroute	Yes
VPLS	No

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 25 on page 30 lists the multicast features that are supported on Junosphere VSRX.

Table 25: Multicast Support

Feature	Junosphere VSRX
Filtering PIM register messages	Yes
IGMP	Yes
PIM RPF routing table	Yes
Primary routing mode (dense mode for LAN and sparse mode for WAN)	Yes
Protocol Independent Multicast Static RP	Yes
Session Announcement Protocol (SAP)	Yes
SDP	Yes

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 26 on page 30 lists the multicast VPN features that are supported on Junosphere VSRX.

Table 26: Multicast VPN Support

Feature	Junosphere VSRX
Basic multicast features in C-instance	Yes
Multicast VPN membership discovery with BGP	Yes
P2MP LSP support	Yes

Table 26: Multicast VPN Support *(continued)*

Feature	Junosphere VSRX
P2MP OAM - P2MP LSP ping	Yes
Reliable multicast VPN routing information exchange	Yes

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, hide topology, and so on.

Table 27 on page 31 lists the NAT features that are supported on Junosphere VSRX.

Table 27: NAT Support

Feature	Junosphere VSRX
Destination IP address translation	Yes
Disabling source NAT port randomization	Yes
Interface source NAT pool port	Yes
NAT address pool utilization threshold status	Yes
NAT traversal (NAT-T) for site-to-site IPsec VPNs (IPv4)	Yes
Persistent NAT	Yes
Persistent NAT binding for wildcard ports	Yes
Persistent NAT hairpinning	Yes
Maximize persistent NAT bindings	Yes
Pool translation	Yes
Proxy ARP (IPv4)	Yes
Proxy NDP (IPv6)	Yes
Removing persistent NAT query bindings	Yes
Rule-based NAT	Yes

Table 27: NAT Support *(continued)*

Feature	Junosphere VSRX
Rule translation	Yes
Source address and group address translation for multicast flows	Yes
Source IP address translation	Yes
Static NAT	Yes

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 28 on page 32 lists the network operations features that are supported on Junosphere VSRX.

Table 28: Network Operations and Troubleshooting Support

Feature	Junosphere VSRX
Event policies	Yes
Event scripts	Yes
Operation scripts	Yes
XSLT commit scripts	Yes

Network Time Protocol

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.

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.

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 29 on page 33 lists the RPM probe features that are supported on Junosphere VSRX.

Table 29: RPM Probe Support

Feature	Junosphere VSRX
RPM probe	Yes
One-way timestamps	Yes

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 prefixes 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 30 on page 33 lists the routing features that are supported on Junosphere VSRX.

Table 30: Routing Support

Feature	Junosphere VSRX
BGP	Yes

Table 30: Routing Support *(continued)*

Feature	Junosphere VSRX
BGP extensions for IPv6	Yes
Compressed Real-Time Transport Protocol (CRTP)	Yes
ECMP flow-based forwarding	Yes
Internet Group Management Protocol (IGMP)	Yes
IPv4 options and broadcast Internet diagrams	Yes
IPv6 routing, forwarding, global address configuration, and Internet Control Message Protocol (ICMP)	Yes
IS-IS	Yes
Multiple virtual routers	Yes
Neighbor Discovery Protocol and Secure Neighbor Discovery Protocol	Yes
OSPF v2	Yes
OSPF v3	Yes
RIP next generation (RIPng)	Yes
RIP v1, v2	Yes
Static routing	Yes
Virtual Router Redundancy Protocol (VRRP)	Yes

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 the 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 31 on page 35 lists the secure web access features that are supported on Junosphere VSRX.

Table 31: Secure Web Access Support

Feature	Junosphere VSRX
CAs	Yes
HTTP	Yes
HTTPS	Yes

Security Policy Support

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 32 on page 35 lists the security policy features that are supported on Junosphere VSRX.

Table 32: Security Policy

Feature	Junosphere VSRX
Address books/Address sets	Yes
Custom policy applications	Yes
Global Policy	Yes
Policy application timeouts	Yes
Policy applications and application sets	Yes
Policy hit-count tracking	Yes
Schedulers	Yes
Security policies for self-traffic	Yes
SSL proxy	No
User role firewall	No
Common predefined applications	Yes
Shadow policy	Yes

Security Zone

A *security zone* is:

- A collection of one or more network segments requiring the regulation of inbound and outbound traffic through policies
- A group of networks that follow the same security principles
- A group of 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.

Table 33 on page 36 lists the zones supported on Junosphere VSRX.

Table 33: Zones Support

Feature	Junosphere VSRX
Functional zone	Yes
Security zone	Yes

Session Logging

You can obtain information about the sessions and packet flows active on your device, including detailed information about specific sessions. You can display this information to observe activity and for debugging purposes.

Table 34 on page 36 lists the session logging features that are supported on Junosphere VSRX.

Table 34: Session Logging Support

Feature	Junosphere VSRX
Accelerating security and traffic logging	Yes
Aggressive session aging	Yes
Getting information about sessions	Yes
Logging to a single server	Yes
Session logging with NAT information	Yes

SMTP

SMTP is used for sending e-mail messages between servers. SMTP can be used to send an e-mail message to a local or a remote mail server to forward an e-mail message. While electronic mail servers use SMTP to send and receive mail messages, user-level client mail applications typically use SMTP only for sending messages to a mail server for relaying. For receiving messages, client applications usually use either Post Office Protocol (POP) or Internet Message Access Protocol (IMAP).

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 to evaluate the overall health of the network and identify bottlenecks.

SNMP v1, v2, and v3 are supported on Junosphere VSRX.

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 35 on page 37 lists the features of stateless firewall filters that are supported on Junosphere VSRX.

Table 35: Stateless Firewall Filters Support

Feature	Junosphere VSRX
Stateless firewall filters (ACLs)	Yes
Stateless firewall filters (simple filter)	No

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 36 on page 38 lists the features of system log files that are supported on Junosphere VSRX.

Table 36: System Log Files Support

Feature	Junosphere VSRX
Archiving system logs	Yes
Configuring system log messages	Yes
Disabling system logs	Yes
Filtering system log messages	Yes
Multiple system log servers (control-plane logs)	Yes
Sending system log messages to a file	Yes
Sending system log messages to a user terminal	Yes
Viewing data plane logs	Yes
Viewing system log messages	Yes

Upgrading and Rebooting

When you power on the Junosphere VSRX VM, it starts (boots up) using its primary boot device. 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 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 files for troubleshooting.

Table 37 on page 38 lists the upgrading and rebooting features that are supported on Junosphere VSRX.

Table 37: Upgrading and Rebooting Support

Feature	Junosphere VSRX
Autorecovery	Yes
Boot device configuration	Yes
Boot device recovery	Yes
Chassis components control	Yes

Table 37: Upgrading and Rebooting Support *(continued)*

Feature	Junosphere VSRX
Chassis restart	Yes
Download manager	Yes
Dual-root partitioning	No
In-band cluster upgrade	No
Low-impact cluster upgrades	No
Software upgrades and downgrades	Yes

User Interfaces

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

The Junos OS CLI is the software interface you use to access a device running Junos OS—whether from the console or through a network connection. By leveraging industry-standard tools and utilities, the CLI provides a powerful set of commands that you can use to monitor and configure devices running Junos OS.

The J-Web interface allows you to monitor, configure, troubleshoot, and manage the routing platform by means of a Web browser enabled with Hypertext Transfer Protocol (HTTP) or HTTP over Secure Sockets Layer (HTTPS). J-Web provides access to all the configuration statements supported by the routing platform, so you can fully configure your device without using the Junos OS CLI.

Table 38 on page 39 lists the user interface features that are supported on Junosphere VSRX.

Table 38: User Interfaces Support

Feature	Junosphere VSRX
CLI	Yes
J-Web user interface	Yes
Junos XML protocol	Yes
Network and Security Manager	No
Junos Space SD	Yes
SRC application	No

PART 2

Index

Index