Junos OS Release 18.2R1 for vSRX Release Notes

Release 18.2R1
28 June 2018
Revision 1

Contents

Introduction

This release note accompanies Junos OS Release 18.2R1 for vSRX. It describes new and changed features, known behavior, and known and resolved problems in the software.

vSRX is a virtual security appliance that provides security and networking services in virtualized private or public cloud environments. It runs as a virtual machine (VM) on x86 servers that support virtualization, and it enables advanced security and routing at the network edge in multitenant virtualized environments.

vSRX is built on Junos OS and delivers security and networking features similar to those available on SRX Series Services Gateways.

You can also find the vSRX release notes in the Juniper Networks TechLibrary, located at https://www.juniper.net/documentation/.

New and Changed Features

This section describes new features and enhancements to existing features in Junos OS Release 18.2R1 for vSRX.

New Features for Junos OS Release 18.2R1 for vSRX

This section describes new features and enhancements to existing features in Junos OS Release 18.2R1 for vSRX.

Application Security

- **Support for Advanced policy-based routing (APBR) policy (SRX Series, vSRX Instances)**—Starting in Junos OS Release 18.2R1, you can configure advanced policy-based routing (APBR) policies by defining source address, destination address, and applications as match conditions; and after a successful match, the configured APBR profile is applied as application services for the session.

  In previous releases of Junos OS, an APBR profile could be attached to an incoming security zone of the ingress traffic, and the APBR was applied only on the basis of the security zone.

  This enhancement provides more flexible traffic-handling capabilities that offer granular control for forwarding packets.

  [See Advanced Policy-Based Routing.]

Application and Access Control

- **Support for User Firewall to configure ClearPass and JIMS at the same time (SRX Series, vSRX)** —Starting in Junos OS Release 18.2R1, you can configure ClearPass and Juniper Identity Management Service (JIMS) at the same time. By configuring ClearPass and JIMS at the same time, SRX Series devices can query JIMS for user identification entries, and ClearPass can push device entries to the SRX Series device through the Web API. In releases before Junos OS Release 18.2R1, you are restricted to configure either ClearPass or JIMS.

  [See Understanding how ClearPass and JIMS works at the same time .]

CoS

- **vSRX: Policer and shaper adjustment per interface** —Starting in Junos OS Release 18.2R1, a vSRX instance now supports a Layer 2 overhead configuration for policer and shaper adjustments. New commands have been added in Junos OS to support this feature on a vSRX:

  NOTE: Only the **interface-specific** filter and **logical-interface-policer** policer are supported.

  - New command for shaping overhead per interface: **set class-of-service interfaces ge-0/0/0 interface-name shaping-rate overhead <bytes>**
  - New commands for policer overhead per interface:
    - **set interfaces ge-0/0/0 interface-name policer-overhead <bytes>**
    - **set interfaces ge-0/0/0 interface-name policer-overhead ingress <bytes>**
    - **set interfaces interface-name policer-overhead egress <bytes>**
    - **set interfaces interface-name policer-overhead egress <bytes>**

[See interfaces (CoS Interfaces).]

Security Policies

- **Support for unified policies (SRX Series, vSRX)**—Starting in Junos OS Release 18.2R1, unified policies are now supported on all SRX Series devices, allowing granular control and enforcement of dynamic Layer 7 applications within the traditional security policy.

  Unified policies are the security policies, where you can use dynamic applications as match conditions along with existing 5-tuple or 6-tuple matching conditions (with user firewall) to detect application changes over time, and allow you to enforce a set of rules for the transit traffic.

  Unified policies allow you to use dynamic application as one of the policy match criteria rule in each application. Application identification (AppID) is applied on the traffic, and the application is identified after several packets are checked.

  Before identifying the final application, the policy cannot be matched precisely. A potential policy list is made available, and the traffic is permitted using the potential policy from the list.

  After the application is identified, the final policy is applied to the session. Policy actions such as permit, deny, reject, or redirect is applied on the traffic as per the policy rules.

  The following features support unified policies:

  - **Application Identification (AppID)**—Unified policy leverages the application identity information from the Application Identification (AppID). AppID provides the information such as dynamic application classification, default protocol and port of an application. For any application included in the dependent list of another application, AppID provides this information.

    [See Application Identification Support for Unified Policies.]

  - **Application firewall (AppFW)**—Unified policy configuration handles AppFW functionality and simplifies the task of configuring firewall policy to permit or block application traffic from the network.

    If you configure a unified policy with a dynamic application as one of the matching conditions, then the configuration eliminates the additional steps involved in AppFW configuration—that is, configuring a security policy to invoke the application firewall service.

    Starting in Junos OS Release 18.2R1, the Application Firewall (AppFW) functionality is deprecated— rather than immediately removed—to provide backward compatibility and a chance to bring your configuration into compliance with the new configuration.

    The **[edit security application-firewall]** hierarchy and all configuration options under this hierarchy are deprecated.

  - **Application Quality of Service (AppQoS)**—AppQoS functionality is supported when the device is configured with unified policies. You can configure a default AppQoS rule set to manage unified policy conflicts, if multiple security policies match the traffic.

- **ICAP service redirect**—Internet Content Adaptation Protocol (ICAP) service redirect functionality is supported when the device is configured with unified policies.
- **IDP**—Starting with Junos OS Release 18.2R1, with unified policies support, when a security rule has IDP enabled, the name of the actual IDP policy is replaced. This is to simplify IDP policy usage and to provide flexibility to have multiple policies active at the same time.

  All IDP matches will now be handled within the unified policies. As a part of session interest check IDP will enabled if IDP policy is present in any of the matched rules.

  IDP policy is activated in security policies, by permitting the IDP policy within the application services using the **set security policies from-zone zone-name to-zone zone-name policy policy-name then permit application-services idp-policy idp-policy-name** command.

  Since IDP policy name is directly use in the security policy rule, the **[edit security idp active-policy policy-name]** statement is deprecated.
- **SSL proxy**—SSL proxy functionality is supported when the device is configured with unified policies. You can configure a default SSL proxy profile to manage unified policy conflicts, if multiple security policies match the traffic.
- **UTM**—A new dynamic-application policy match condition is added to SRX Series devices, allowing an administrator to more effectively control the behavior of Layer 7 applications. To accommodate Layer 7 application-based policies in UTM, the **[edit security utm default-configuration]** command is introduced. If any parameter in a specific UTM feature profile configuration is not configured, then the corresponding parameter from the UTM default configuration is applied.

  Additionally, during the initial policy lookup phase which occurs prior to a dynamic application being identified, if there are multiple policies present in the potential policy list which contains different UTM profiles, the SRX Series device applies the default UTM profile until a more explicit match has occurred.

[See Unified threat management (UTM) support within Unified Policy.]

VPN

- **Configuring forwarding class on IPsec VPNs (SRX Series, vSRX instances)**—Starting in Junos OS Release 18.2R1, forwarding classes configured on an SRX Series device or vSRX instance can be mapped to IPsec security associations (SAs). Multiple IPsec SAs are negotiated on the same IKE SA with a peer device, one SA per forwarding class configured in IPsec.

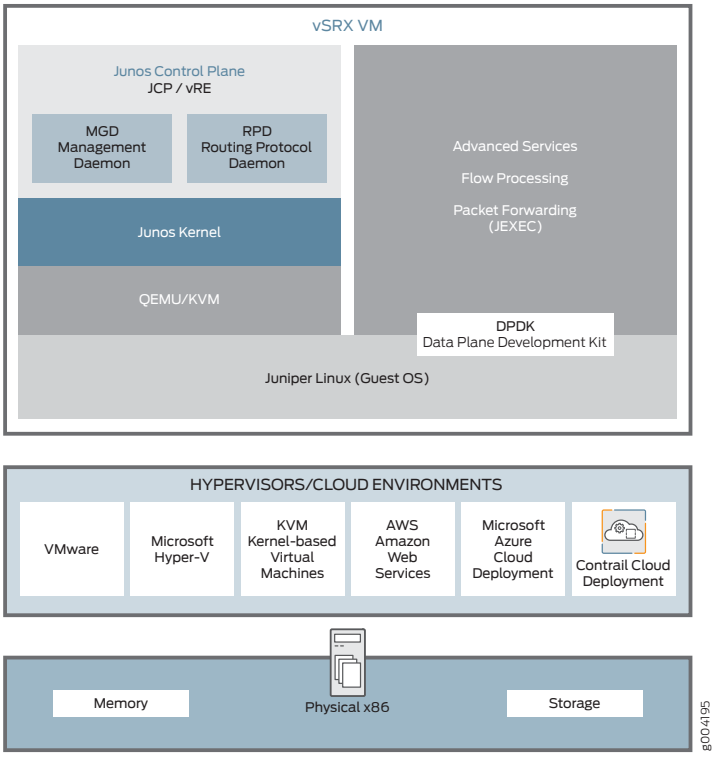
  A unique IPsec SA is negotiated with the VPN peer for each forwarding class. By mapping the forwarding class to the IPsec SA, all the packets with a certain class-of-service (CoS) value will get quality-of-service (QoS) treatment between the peer devices, avoiding packet drop due to the anti-replay window. This feature provides QoS for IPsec when peer devices allow for multiple SA negotiation.

vSRX Architecture Illustration

vSRX Architecture

Figure 1 on page 7 is a high-level illustration of the vSRX architecture as of Junos OS Release 18.2R1.

Figure 1: vSRX Architecture



Supported Features

For details about Junos OS features supported on vSRX, see Feature Explorer: vSRX.

Supported Features References

Table 1 on page 8 lists documentation references to Junos OS features that are supported on vSRX.

NOTE: Some vSRX features require a license. See vSRX Feature Licenses Overview for more details.

Table 1: Documentation References for Junos OS Features Supported on vSRX

Feature	Feature Documentation	vSRX Platform
Application Firewall (AppFW)	Application Firewall Overview	VMware, KVM, Contrail, AWS, Azure, and Hyper-V
Application Identification (AppID)	Understanding Application Identification Techniques	VMware, KVM, Contrail, AWS, Azure, and Hyper-V
Application Layer Gateways (ALGs)	ALG Overview	VMware, KVM, Contrail, AWS, Azure, and Hyper-V
Application Quality of Service (AppQoS)	Understanding Application QoS (AppQoS)	VMware, KVM, Contrail, AWS, Azure, and Hyper-V
Attack Detection and Prevention (ADP)	Attack Detection and Prevention Overview	VMware, KVM, Contrail, AWS, Azure, and Hyper-V
Chassis cluster support for Virtio driver	Chassis Cluster Overview	KVM
Chassis cluster support for VMXNET3 driver	Chassis Cluster Overview	VMware
Chassis cluster support for Windows Hyper-V Server 2016	Chassis Cluster Overview	Hyper-V
Class of service (CoS)	Understanding Class of Service	VMware, KVM, Contrail, AWS, Azure, and Hyper-V
Dynamic Host Configuration Protocol (DHCP)	Understanding Interfaces	VMware, KVM, Contrail, AWS, Azure, and Hyper-V
Flow and packet processing	Juniper Networks Devices Processing Overview	VMware, KVM, Contrail, AWS, Azure, and Hyper-V

Table 1: Documentation References for Junos OS Features Supported on vSRX (continued)

Feature	Feature Documentation	vSRX Platform
Intrusion Detection and Prevention (IDP)	Understanding Intrusion Detection and Prevention	VMware, KVM, Contrail, AWS, Azure, and Hyper-V
IPsec VPN	IPsec VPN Overview	VMware, KVM, Contrail, AWS, Azure, and Hyper-V
Multiprotocol Label Switching (MPLS)	MPLS Overview	VMware, KVM, Contrail, AWS, Azure, and Hyper-V
Multicast	Multicast Overview	VMware, KVM, and Contrail
Network Address Translation (NAT)	Introduction to NAT	VMware, KVM, Contrail, AWS, Azure, and Hyper-V
Routing protocols	Junos OS Routing Protocols Library	VMware, KVM, Contrail, AWS, Azure, and Hyper-V
Security building bocks	Understanding Security Basics	VMware, KVM, Contrail, AWS, Azure, and Hyper-V
Transparent mode	Ethernet Switching and Layer 2 Transparent Mode Overview	VMware, KVM, and Contrail
Unified Threat Management (UTM)	Unified Threat Management Overview	VMware, KVM, Contrail, AWS, Azure, and Hyper-V
User authentication	Understanding User Authentication for Security Devices	VMware, KVM, Contrail, AWS, Azure, and Hyper-V

Unsupported Features

While vSRX supports many of the Junos OS features supported on other SRX Series devices, not all features are supported. For information about Junos OS features that are not supported on vSRX, see "Known Behavior" on page 12 and SRX Series Features Not Supported on vSRX for specific support limitations.

Changes in Behavior and Syntax

This section lists the changes in behavior of Junos OS features and changes from Junos OS Release 18.2R1 for the vSRX. For the most complete and latest information about changes in command behavior and syntax applicable to all SRX Series platforms in Junos OS Release 18.2R1, see Changes in Behavior and Syntax for SRX.

Application System Cache for Application Services (SRX Series, vSRX Instances)

Starting with Junos OS 18.2R1, the default behavior of the ASC has changed as follows:

- Security services such as security policies, application firewall (AppFW), Juniper Sky ATP, IDP, and UTM do not use the ASC by default.
- Miscellaneous services such as APBR and AppTrack use the ASC for application identification by default.

NOTE: The change in the default behavior of the ASC affects the legacy Application Firewall (AppFW) functionality. With the ASC disabled by default for the security services starting in Junos OS Release 18.2 onwards, the AppFW will not use the entries present in the ASC.

You can revert to the ASC behavior as in Junos OS releases prior to 18.2 by using the **set services application-identification application-system-cache security-services** command.

CAUTION: The SRX Series device may become susceptible to application evasion techniques if the ASC is enabled for security services. We recommend that you enable the ASC only when the performance of the device in its default configuration (disabled for security services) is not sufficient for your specific use case.

Use the following commands to enable or disable the ASC:

- Enable the ASC for security services:

  user@host# set services application-identification application-system-cache security-services

- Disable the ASC for miscellaneous services:

  user@host# set services application-identification application-system-cache no-miscellaneous-services

- Disable the enabled ASC for security services:

  user@host# delete services application-identification application-system-cache security-services

- Enable the disabled ASC for miscellaneous services:

  user@host# delete services application-identification application-system-cache no-miscellaneous-services

You can use the **show services application-identification application-system-cache** command to verify the status of the ASC.

The following sample output provides the status of the ASC:

```
user@host>show services application-identification application-system-cache
Application System Cache Configurations:
  application-cache: on
```

```
  Cache lookup for security-services: off
  Cache lookup for miscellaneous-services: on
cache-entry-timeout: 3600 seconds
```

For Junos OS Release prior to 18.2R1, application caching is turned on by default. You can manually turn this caching off using the CLI.

```
user@host# set services application-identification no-application-system-cache
```

Known Behavior

This section contains the known behaviors, system maximums, and limitations in hardware and software in Junos OS Release 18.2R1 for vSRX.

Chassis Cluster/High Availability

- In vSRX deployments, HA is not supported on AWS and Microsoft Azure.
- In KVM deployments using Virtio, when vSRX is operating in HA and sessions are established and closed at very high rates, some sessions might not get closed on the backup node. This issue is because of a Virtio driver limitation.

  Workaround: Reduce session establish rate to less than 300 cps.
- In KVM deployments using Virtio, when vSRX is operating in HA, packet loss is observed during an RG0 failover. This occurs because the MAC entry at the bridge layer cannot be updated by the HA mechanism because of a driver limitation. Packets must remain in the queue until they expire.

Interfaces and Routing

- In vSRX deployments, source MAC filtering is supported on Fast Ethernet and Gigabit Ethernet interfaces in Layer 3 standalone mode and redundant Ethernet interfaces in HA mode. However, support is not available on Aggregated Ethernet (AE), Fabric Ethernet, or Gigabit Ethernet interfaces in Layer 2 standalone mode.
- In vSRX deployments, the following configuration options are not supported: *services unified-access-control* and *protocols l2-learning global-mode switching*.
- In vSRX deployments, configuring XAuth with AutoVPN secure tunnel (st0) interfaces in point-to-multipoint mode and dynamic IKE gateways is not supported. However, XAuth is supported with shared IKE IDs.
- In vSRX deployments using VMware ESX, changing the default speed (1000 Mbps) or the default link mode (full duplex) is not supported on VMXNET3 vNICs.

Platform and Infrastructure

- VRRP is not supported on VMware hypervisors because of a VMware support limitation for virtual MAC addresses.
- In VMware deployments, a serial console port on the vSRX platform cannot be used through the network to redirect console messages to a telnet session because of an

underlying infrastructure limitation. The console port can be configured; however, it is not usable.

- In a vSRX deployment in VMware ESXi 5.5 using VMXNET3 vNICs, a performance degradation (8 percent) is observed when more vNICs (approximately eight) are configured, compared with fewer vNICs (approximately three) across a single instance.
- DPDK does not provide an outgoing multicast traffic count on its interface. As a result, interface outgoing multicast packets are interpreted as incoming packets on the egress interface.
- In vSRX deployments, the vSRX VM does not support the use of Live Migration or vMotion as a means to move virtual machines from one host to another.

NFX Platform

- When vSRX is run as a virtual network function (VNF) on the NFX250 Network Services Platform, for the vSRX Junos OS release, whenever a new vSRX instance is created the boot-up time for the vSRX increases by approximately four minutes as compared with the Junos OS 15.1X49-D78.4 version of vSRX. Whenever the same vSRX instance is deleted and redeployed on the device using the same qcow image, then the boot-up time is one minute more than that of Junos OS 15.1X49-D78.4 version of vSRX.

SR-IOV

- SR-IOV interfaces have both physical functions (PFs) and multiple virtual functions (VFs). When configuration parameters are modified on the VF, the PF driver has the option to accept or reject the change. As a security precaution, the generic PF driver that is part of standard hypervisors (both VMware and Linux) does not allow certain parameters to be configured. Parameters that cannot be changed include enabling promiscuous mode, enabling multicast, and allowing Jumbo frames. Because of this driver limitation, the following vSRX features are not supported in deployments that use SR-IOV interfaces:
  - High availability (HA)
  - IRB interfaces
  - IPv6 addressing
  - Jumbo frames
  - Layer 2 support
  - Multicast with other features such as OSPF and IPv6
  - Packet mode

  These limitations apply in deployments where the PF drivers cannot be updated or controlled. The limitations do not apply when vSRX is deployed on supported Juniper Networks devices.
- SR-IOV does not support all VMware features (see your VMware documentation).
- In either a Microsoft Azure or Microsoft Hyper-V deployment, SR-IOV is not supported.

- Cloning vSRX VMs with SR-IOV interfaces is not supported. Instead of cloning a VM, instantiate a new vSRX VM from the .ova image (VMware hypervisors) or from the .qcow2 image (KVM hypervisors).
- In deployments using SR-IOV interfaces, Address Resolution Protocol (ARP) does not work when Jumbo frames are used on a physical NIC.
- In deployments using SR-IOV interfaces, packets are dropped when a MAC address is assigned to a vSRX Junos OS interface. This issue occurs because SR-IOV does not allow MAC address changes in either the PF or the VF.
- In KVM deployments using SR-IOV interfaces with a DPDK driver, the PF interface might go down and then come back up. In such circumstances, the vSRX might stay down even after the PF is back up because the Junos OS ge- interface does not receive an updated link state message from the VF interface.

  Workaround: Reboot the vSRX instance.
- In KVM deployments operating in SR-IOV mode with an Intel X710/XL710 NIC, note that there is no VLAN support for the vSRX interfaces in this configuration. This is due to an Intel card limitation with the X710 and XL710 NICs.

vSRX Limitations in Junos Space Security Director Integration with vSRX

The following vSRX features are not supported in Security Director:

- Application QoS (AppQoS)
- Layer 2 transparent mode
- Specific Security Director limitations with respect to Application Firewall (AppFW), IDP, and UTM features:
  - UTM database updates are not supported.
  - Application ID (AppID) custom signatures are not supported.
- The following vSRX features are not supported in Junos Space Security Director for IPsec and routing features:
  - Certificates for AutoVPN must be generated from the CLI.
  - All other IPsec settings can be configured using Junos Space Security Director.

Known Issues

This section lists the known issues in Junos OS Release 18.2R1 for vSRX.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

Chassis Clustering

- In HA deployments, when the Routing Engine is busy and an RG0 manual failover is initiated, a control link failure occurs. A failed control link causes both control link detection methods (tcp keepalive and control link heart beat) to fail; it also results in an RG1+ failover. This situation might eventually lead to an RG1+ split brain condition. PR1085987
- In a cluster environment, when the primary node is shut down on VMware ESXi by the vSphere client, the remaining node state transitions from *Secondary* to *Ineligible* before changing to the *Primary* state. This change in state change can lengthen the delay to failover. PR1216447
- The vSRX HA control link might go down under high-traffic conditions, which disables the secondary node. PR1229172
- With vSRX instances running in a chassis cluster, when rebooting the primary node for redundancy-group 1+, traffic forwarding may stop for approximately a minute. PR1258502

  Workaround: First manually failover redundancy-group 1+ before rebooting a cluster node.
- A high-availability cold-sync failure might occur when using PCI passthrough as FAB. When this issue occurs, the vSRX might become unresponsive. PR1263056

  Workaround: Perform a manual failover for redundancy-group 1+ before rebooting a cluster node. If this does not resolve the issue, use Virtio as FAB.
- When operating in a high-availability environment using the vSRX3.0 image, when a device boots up as secondary node, in some instances the application-package fails to be auto-installed. This can be manually downloaded and installed using CLI commands. PR1363431

Class of Service (CoS)

- On vSRX instances when classifiers, schedulers, and shapers are configured, the interface queue counters where these schedulers are applied do not match the expected number of packets. PR1083463

Cloud-init in AWS

- If using cloud-init in AWS to automate the initialization of vSRX instances, when you click **View Instances** to display the Instances list in the EC2 Dashboard, you might find that it takes several minutes to launch the vSRX instance. For the initial boot, the vSRX instance might show an error of “1/2 checks passed” until it initializes, and then finally display “2/2 checks passed.” PR1296704
- If using cloud-init in AWS to automate the initialization of vSRX instances, you might encounter an SSH connection failure if using an incorrect configuration with keywords in the user-data file. PR1297086

Workaround: The configuration must be validated, and include details for the fxp0 interface, login, and authentication. It must also have a default route for traffic on fxp0. This information must match the details of the AWS VPC and subnet into which the instance is launched. If any of this information is missing or incorrect, the instance is inaccessible and you must launch a new one.

In addition, ensure that DHCP server or static IP addressing root-authentication is specified, as well as a default gateway for a static IP address, for the user-data file in AWS.

NOTE: **The user-data file cannot exceed 16 KB. If your user-data file exceeds this limit, you must compress the file using gzip and use the compressed file. For example, the gzip junos.conf command results in the junos.conf.gz file.**

DHCP

- In vSRX deployments, when you exclude an assigned address from the DHCP pool on a DHCP server, the DHCP client gets the excluded address when you use the command **request dhcp client renew all**. This issue occurs because the CLIENT_EVENT_RECONFIGURE event, sent to the client when the **request dhcp client renew** command was issued, is handled by the client in the bound state. This issue is applicable only to DHCPv4 clients.

  Workaround: Clear the binding on the DHCP client by using the **clear dhcp client binding all** command, and then run the **request dhcp client renew all** command to get a new IP address.

  PR1094252

  PR1094257

Flow and Processing

- When vSRX FTP self-traffic crosses a virtual router, the FTP session might fail. PR1079190
- In vSRX deployments, traffic is dropped when a loopback address (lo0.0) and a generic routing encapsulation (GRE) physical interface are configured in different zones. PR1081171

  Workaround: Configure lo0.0 and GRE in the same zone, or use the IP address of the physical interface as the source IP address of the GRE interface.
- Because all DPDK vhost user vNICs on OVS are, by default, bound to the CPUs on Numa node 0, only the OVS poll mode driver (PMD) threads running on node 0 can poll packets on the vhost user NICs. For the performance test to be done on node 1, although you can add the CPU mask to use CPUs on Numa node 0 to poll the packet from the DPDK vhost user NICs, this action can seriously impact performance because of traffic across Numa nodes. PR1241975

Workaround: A solution to this issues consists of two steps:

1. Compile the DPDK with CONFIG_RTE_LIBRTE_VHOST_NUMA enabled:
   /config/common_base:556:CONFIG_RTE_LIBRTE_VHOST_NUMA=y

2. Set the QEMU process to run on the Numa node 1 by adding **emulatorpin** elements to the XML file.

```
<cputune>
    <vcpupin vcpu='0' cpuset='45'/>
    <vcpupin vcpu='1' cpuset='46'/>
    <vcpupin vcpu='2' cpuset='47'/>
    <vcpupin vcpu='3' cpuset='48'/>
    <vcpupin vcpu='4' cpuset='49'/>
    <emulatorpin  cpuset='50-53'/>
 </cputune>
```

Interfaces and Routing

- RSVP neighbors are not established on a VMware ESXi host if NSX components are installed on that host. PR1092514
- On a VMware ESXi host, packets with VLAN do not cross over ESXi hosts when NSX components are installed through a Virtual Extensible LAN (VXLAN) port group. PR1092517
- When running VMware ESXi 5.5.0U3, in the **show chassis fpc detail** output, the current status of fpc0 shows that it is in cluster mode. Normally, the mode is displayed as online. PR1141998

  Workaround: Use VMware ESXi 5.5.0U2 or upgrade to VMware ESXi 6.0.
- When you operate the vSRX in transparent mode with VMware ESXi 5.1 as the host, some packet corruption might occur at the VMXNET3 driver level if TCP segmentation offload (TSO) is enabled on the host. PR1200051

  NOTE: **This issue does not occur with VMware ESXi 5.5 and later.**

  Workaround: Disable TSO in the data path on the VMware ESXi 5.1 host.
- The **monitor traffic** CLI command cannot be used to capture vSRX plain ping-to-host revenue ports traffic. All plain ping packets transmitted to revenue ports are handled on the srxpfe side, and vSRX revenue ports traffic will not be seen by RE using this command. However, traffic coming out from revenue ports can be seen by RE. Revenue ports refer to all ports except fxp0 and em0. PR1234321
- On vSRX, 10-Gigabit Ethernet interfaces are being displayed as 1-Gigabit Ethernet interfaces. PR1236912

  NOTE: **This is a display issue and will be addressed in a future version of Junos OS.**

- When performing a rapid disable interface/enable interface sequence on a vSRX (for example, when using a script), this action might trigger an Intel i40e-based NIC limitation where the NIC becomes unresponsive and is unable to receive packets. PR1253659

  Workaround: If possible, avoid using a script to perform a rapid disable interface/enable interface sequence on the vSRX. If you encounter this issue, login to the host and reload the Intel i40e driver to recover the NIC.

- In some cases, when you specify the **show interfaces gr-0/0/0 statistics detail** command, the show command output under Physical interface does not properly reflect the input and output packets or bytes in the Traffic statistics. PR1292261

- When operating in LDOM mode, the **set protocols router-advertisement** command cannot be configured under logical-systems. PR1331220

  Workaround: Configure the global **set protocols router-advertisement** command.

  NOTE: Note the following usage considerations associated with this workaround:

  - The global configuration is invisible for logical system tenants, so they cannot configure router-advertisement protocols by themselves.
  - The DHCPv6 client in autoconfig mode in logical-systems cannot be configured because it needs ra enabled in logical-systems.

- When operating in LDOM mode, the **policy-option** cannot be configured under logical-systems in logical-domain mode. PR1331232

- In some cases, the DHCP RELEASE packet might not be sent when you specify the **clear dhcp client bindings** command. PR1338001

J-Web

- The addition of a block of 2000+ global addresses at a time to an SSL proxy profile-exempted address might cause the J-Web interface to become unresponsive. PR1278087

  Workaround: Only add 500 global addresses at a time.

- You might encounter issues when you attempt to view custom log files created for event logging in the J-Web interface. Only event logs captured in a policy-session log file can be viewed in the J-Web interface (**Monitor > Events and Alarms > View Events**), and other event logs captured in different files are missing. PR1280857

  Workaround: If this issue occurs, download the custom log file from **Administration > Files > Log Files** so you can properly view them.

- The Applications, Threat Map, and Firewall: Top Denies Dashboard widgets might display **No Data Available** when the device receives a huge amount of data. PR1282666

  Workaround: If this issue occurs, individually refresh each of the Dashboard widgets.

- You are unable to view the Java applet in the Google Chrome web browser when attempting to use the J-Web CLI terminal. The J-Web CLI terminal does not work when using a version of Google Chrome web browser that is greater than version 42.0. PR1283216

  Workaround: To use J-Web CLI terminal, use one of the following recommended web browsers and versions:

  - Google Chrome, version 42.0 or earlier.
  - Microsoft Internet, Explorer version 11 or 10.
  - Firefox, version 46 or later.

- In some cases, when using the Google Chrome web browser, the Time Range slider does not function properly for events. PR1283536

  Workaround: If you encounter this behavior, use the Microsoft Internet Explorer version 11 web browser.

- Uploading a certificate using the **Browse** button stores the certificate in the SRX Series device or vSRX instance at the **/jail/var/tmp/uploads/** location. The certificate will be deleted when you execute the **request system storage cleanup** command. PR1312529

  Workaround: If this issue occurs, perform one of the following actions:

  - Refrain from deleting the certificate while executing the **request system storage cleanup** command. If the certificate is deleted, replace it immediately or the connection to the JIMS server will go down.
  - Save the certificate manually in the SRX Series device or vSRX instance in a location other than **/tmp/** folder. Use the J-Web option **Specify path of the file on device** and specify the correct path.

- The values of address and address-range are not displayed in the Inline address-set creation pop-up window of the JIMS server. PR1312900

  Workaround: To determine the value of the global address, address-set, and address-range values, navigate to **Configure -> Security -> Objects** and access Global addresses.

Microsoft Azure

- Nested vmx (hardware virtualization support) is not supported for a vSRX that is deployed on Microsoft Azure. Please note that this has no impact to vSRX functionality, but it can slightly affect the bootup time and configuration commit time. PR1231270

Microsoft Hyper-V

- When you deploy a vSRX virtual security appliance on Windows Hyper-V Server 2012 (vSRX support for the Hyper-V hypervisor), if the bidirectional traffic of each port exceeds the capability of the vSRX, you might find that one vSRX port hangs and becomes unable to receive packets. PR1250285

  Workaround: Upgrade Windows Hyper-V Server 2012 to Windows Hyper-V Server 2012 R2.

Platform and Infrastructure

- In a KVM-based hypervisor, an attempt to save vSRX and restore it through the Virtual Machine Manager GUI causes the Virtual Routing Engine (VRE) to crash. The crash causes the vRE to go to DB mode. PR1087096

  Workaround: Use either **virsh destroy/start VM** or **nova stop/start/reboot VM** but not the Virtual Machine Manager GUI.

- In KVM deployments, virsh **reset** commands do not work. PR1087112
- The AWS snapshot feature cannot be used to clone vSRX instances. You can use the AWS snapshot feature to preserve the state of the VM so you can return to the same state when the snapshot was created. PR1160582
- vSRX uses DPDK to increase packet performance by caching packets to send in burst mode. Latency-sensitive applications must account for this burst operation. PR1087887
- APIC virtualization (APICv) does not work well with nested VMs such as those used with KVM. On Intel CPUs that support APICv (typically v2 models, for example E5 v2 and E7 v2), you must disable APICv on the host server before deploying vSRX. PR1111582

  Workaround: Disable APICv before deploying vSRX.

  Use the following commands to disable APICv on your host and verify that it is disabled:

  ```
  sudo rmmod kvm-intel
  sudo sh -c "echo 'options kvm-intel enable_apicv=n' >> /etc/modprobe.d/dist.conf"
  sudo modprobe kvm-intel
  root@host:~# cat /sys/module/kvm_intel/parameters/enable_apicv
  N
  ```

- In a KVM-based hypervisor deployment, you might encounter one or more of following issues: PR1263056
  - The vSRX may become unresponsive when Page Modification Logging (PML) is enabled in the host operating system (CentOS or Ubuntu) when using the Intel Xeon Processor E5 or E7 v4 family. This PML issue prevents the vSRX from successfully booting.

- Traffic to the vSRX might drop or stop due to Intel XL710 driver-specific limitations. This behavior can be due to issues with the vSRX VM configuration (such as a MAC-VLAN or MAC-NUM limitation).

Workaround: Perform the appropriate workaround to resolve the issues listed above:

- If the vSRX becomes unresponsive due to a PML issue, we recommend that you disable the PML at the host kernel level. Depending on your host operating system, open the .conf file in your default editor and add the following line to the file: **hostOS# options kvm-intel nested=y enable_apicv=n pml=n**.
- If the vSRX experiences loss of traffic due to Intel XL710 driver limitations, follow the recommended Intel XL710 guidelines to change the VM configuration to avoid these limitations. See Intel Ethernet Controller X710 and XL710 Family Documentation for the recommended guidelines.

Routing Protocols

- When the Bidirectional Forward Detection (BFD) protocol is configured over an IPv6 static route, the route remains in the routing table even after a session failure occurs. PR1109727

UTM

- In vSRX deployments configured with Sophos Antivirus, some files that are larger than the configured **max-content-size** might not go into fallback mode, and, after they are retransmitted several times, they might pass with a clean or an infected result. This issue is specific to a few protocols that do not send the content size before attempting to transmit files. PR1093984
- In some instances, validation is not checked when the UTM policy is detached from the firewall policy rule after an SSL proxy profile is selected. PR1285543

  Workaround: The UTM policy should not be detached after an SSL proxy profile is selected.
- In a configuration where multiple traffic selectors are configured for a peer with Internet Key Exchange version 2 (IKEv2) reauthentication, only one traffic selector will rekey at the time of the IKEv2 reauthentication. The VPN tunnels of the remaining traffic selectors will be cleared without immediately performing the rekey process. A new negotiation of those traffic selectors will trigger through other mechanisms, for example by traffic or by a peer. PR1287168

VPN

- An error message might occur for **show** or **clear** commands if IPsec VPN is configured with over 1000 tunnels. PR1093872

  Workaround: Retry the commands.
- IPv6 firewall filters cannot be applied to virtual channels. PR1182367

- When IPsec is used with PKI authentication, the vSRX might unnecessarily send the entire certificate chain to the remote peer, potentially causing fragmentation of IKE messages. PR1251837

  Workaround: If possible, configure the remote peer to send the CERTREQ (certificate request) payload as part of the IKE exchange. The vSRX will examine the CERTREQ payload from the remote peer to determine what CAs the peer trusts and to compare them with the CAs trusted locally. This examination helps avoid sending the entire certificate chain to the peer.

- When operating in an AutoVPN or ADVPN configuration, when the st0 interface is in P2MP mode with an IPv4 address and with tunnels coming up, changing the st0 IP address from IPv4 to IPv6, or the OSPF configuration to OSPF3 configuration on the st0 interface, committing the new st0 IP changes might fail to bring up the IPv6 tunnels. PR1321033

  Workaround: After changing the st0 IP address (for example, from IPv4 to IPv6), perform one of the following workarounds to bring up the tunnels:

  - Deactivate, and then activate the VPN object.
  - Specify the **load override** command to completely replace the current candidate configuration with the file you are loading.
  - Perform a **commit full** to check and evaluate the new configuration. A **commit full** is useful for if you get an error with commit or when you have changed the configuration significantly.

Resolved Issues

This section lists the issues that have been fixed in the Junos OS Release 18.2R1.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

Licensing

- On all SRX models, including vSRX instance, in rare cases you might find that the routing engine CPU utilization becomes high after renewing a license key. PR1325236

Interfaces and Routing

- The minimum **source-threshold** and **destination-threshold** value for **tcp syn-flood** in the **set security screen ids-option** command has changed from 1 to 4. PR1349327

Platform and Infrastructure

- During an upgrade from Junos OS 17.3R1 to 17.4R1, if there is a specific AppSecure configuration, configuration errors might prevent HA cluster devices from booting up normally. PR1317563
- The **request message all message** command does not work properly when executed using REST API because the vSRX instance does not support the XML equivalent of the remote procedure call (RPC) command. PR1324627

  The vSRX instance now supports the following new XML tag to support the RPC command:
  <rpc><request-message-all><message>test</message></request-message-all></rpc>.
- On vSRX instances, and SRX1500, SRX4100, and SRX4200 Series devices, you might find that NTP synchronization fails after a period of time and switches to the local clock.PR1331444
- When deploying a vSRX instance in a KVM or Contrail environment with the vhost_net NIC driver, the vSRX might process and forward all unicast packets which were flooded to the port, regardless of the destination MAC address. PR1344700

Routing Policy and Firewall Filters

- On all SRX models, including vSRX instances, when source address is configured for a name-server configuration, the source address is not actually used for the DNS lookup. In addition, the security dns-cache table will not be populated, and security policies are unable to use the FQDN addresses. PR1328925

Migration, Upgrade, and Downgrade Instructions

This section contains information about how to upgrade Junos OS for vSRX using the CLI. Upgrading or downgrading Junos OS can take several hours, depending on the size and configuration of the network.

You also can upgrade to Junos OS Release 18.2R1 for vSRX using J-Web (see J-Web) or the Junos Space Network Management Platform (see Junos Space).

NOTE: You can also upgrade to Junos OS 18.2R1 from Junos OS 15.1X49-D15 or later.

Upgrading Software Packages

To upgrade the software using the CLI:

1. Download the Junos OS Release 18.2R1 for vSRX .tgz file from the Juniper Networks website. Note the size of the software image.

2. Verify that you have enough free disk space on the vSRX to upload the new software image.

```
root@vsrx> show system storage
Filesystem              Size       Used      Avail  Capacity   Mounted on
/dev/vtbd0s1a           694M       433M       206M       68%  /
devfs                   1.0K       1.0K         0B      100%  /dev
/dev/md0                1.3G       1.3G         0B      100%  /junos
/cf                     694M       433M       206M       68%  /junos/cf
devfs                   1.0K       1.0K         0B      100%  /junos/dev/
procfs                  4.0K       4.0K         0B      100%  /proc
/dev/vtbd1s1e           302M        22K       278M        0%  /config
/dev/vtbd1s1f           2.7G        69M       2.4G        3%  /var
/dev/vtbd3s2             91M       782K        91M        1%  /var/host
/dev/md1                302M       1.9M       276M        1%  /mfs
/var/jail               2.7G        69M       2.4G        3%  /jail/var
/var/jails/rest-api       2.7G        69M       2.4G       3%  /web-api/var
/var/log                2.7G        69M       2.4G       3%  /jail/var/log
devfs                   1.0K       1.0K         0B      100%  /jail/dev
192.168.1.1:/var/tmp/corefiles       4.5G       125M       4.1G     3%
/var/crash/corefiles
192.168.1.1:/var/volatile       1.9G       4.0K       1.9G     0%
/var/log/host
192.168.1.1:/var/log       4.5G       125M       4.1G     3%
/var/log/hostlogs
192.168.1.1:/var/traffic-log       4.5G       125M       4.1G     3%
/var/traffic-log
192.168.1.1:/var/local       4.5G       125M       4.1G     3%  /var/db/host
192.168.1.1:/var/db/aamwd       4.5G       125M       4.1G     3%
/var/db/aamwd
192.168.1.1:/var/db/secinteld       4.5G       125M       4.1G     3%
/var/db/secinteld
```

3. Optionally, free up more disk space if needed to upload the image.

```
root@vsrx> request system storage cleanup

List of files to delete:

  Size Date    Name
    11B Sep 25 14:15 /var/jail/tmp/alarmd.ts
 259.7K Sep 25 14:11 /var/log/hostlogs/vjunos0.log.1.gz
   494B Sep 25 14:15 /var/log/interactive-commands.0.gz
  20.4K Sep 25 14:15 /var/log/messages.0.gz
    27B Sep 25 14:15 /var/log/wtmp.0.gz
    27B Sep 25 14:14 /var/log/wtmp.1.gz
```

```
  3027B Sep 25 14:13 /var/tmp/BSD.var.dist
     0B Sep 25 14:14 /var/tmp/LOCK_FILE
   666B Sep 25 14:14 /var/tmp/appidd_trace_debug
     0B Sep 25 14:14 /var/tmp/eedebug_bin_file
    34B Sep 25 14:14 /var/tmp/gksdchk.log
    46B Sep 25 14:14 /var/tmp/kmdchk.log
    57B Sep 25 14:14 /var/tmp/krt_rpf_filter.txt
    42B Sep 25 14:13 /var/tmp/pfe_debug_commands
     0B Sep 25 14:14 /var/tmp/pkg_cleanup.log.err
    30B Sep 25 14:14 /var/tmp/policy_status
     0B Sep 25 14:14 /var/tmp/rtsdb/if-rtsdb
Delete these files ? [yes,no] (no) yes
<output omitted>
```

NOTE: If this command does not free up enough disk space, see [SRX] Common and safe files to remove in order to increase available system storage for details on safe files you can manually remove from vSRX to free up disk space.

4. Use FTP, SCP, or a similar utility to upload the Junos OS Release 18.2R1 for vSRX .tgz file to **/var/crash/corefiles/** on the local file system of your vSRX VM. For example:

```
root@vsrx> file copy ftp://username:prompt@ftp.hostname.net/pathname/
junos-vsrx-x86-64-18.2-2018-2-10.0_RELEASE_182_THROTTLE.tgz
/var/crash/corefiles/
```

5. From operational mode, install the software upgrade package:

```
root@vsrx> request system software add
/var/crash/corefiles/junos-vsrx-x86-64-18.2-2018-2-10.0_RELEASE_182_THROTTLE.tgz
 no-copy no-validate reboot

Verified junos-vsrx-x86-64-18.2-2018-2-10.0_RELEASE_182_THROTTLE signed by
 PackageDevelopmentEc_2017 method ECDSA256+SHA256
THIS IS A SIGNED PACKAGE

WARNING:     This package will load JUNOS 18.2 software.
WARNING:     It will save JUNOS configuration files, and SSH keys
WARNING:     (if configured), but erase all other files and information
WARNING:     stored on this machine.  It will attempt to preserve dumps
WARNING:     and log files, but this can not be guaranteed.  This is the
WARNING:     pre-installation stage and all the software is loaded when
WARNING:     you reboot the system.

Saving the config files ...
Pushing Junos image package to the host...
Installing
/var/tmp/install-media-srx-mr-vsrx-18.2-2018-2-10.0_RELEASE_182_THROTTLE.tgz
Extracting the package ...
total 975372
-rw-r--r-- 1 30426 950 710337073 Oct 19 17:31
junos-srx-mr-vsrx-18.2-2018-2-10.0_RELEASE_1821_THROTTLE-app.tgz
-rw-r--r-- 1 30426 950 288433266 Oct 19 17:31
junos-srx-mr-vsrx-18.2-2018-2-10.0_RELEASE_182_THROTTLE-linux.tgz
Setting up Junos host applications for installation ...

==========================================
```

```
Host OS upgrade is FORCED
Current Host OS version: 3.0.4
New Host OS version: 3.0.4
Min host OS version required for applications: 0.2.4
==========================================

Installing Host OS ...
upgrade_platform: --------------------
upgrade_platform: Parameters passed:
upgrade_platform: silent=0
upgrade_platform:
package=/var/tmp/junos-srx-mr-vsrx-18.2-2018-2-10.0_RELEASE_182_THROTTLE-linux.tgz
upgrade_platform: clean install=0
upgrade_platform: clean upgrade=0
upgrade_platform: Need reboot after staging=0
upgrade_platform: --------------------
upgrade_platform:
upgrade_platform: Checking input
/var/tmp/junos-srx-mr-vsrx-18.2-2018-2-10.0_RELEASE_182_THROTTLE-linux.tgz
 ...
upgrade_platform: Input package
/var/tmp/junos-srx-mr-vsrx-18.2-2018-2-10.0_RELEASE_182_THROTTLE-linux.tgz
 is valid.
upgrade_platform: Backing up boot assets..
cp: omitting directory '.'
bzImage-intel-x86-64.bin: OK
initramfs.cpio.gz: OK
version.txt: OK
initrd.cpio.gz: OK
upgrade_platform: Checksum verified and OK...
/boot
upgrade_platform: Backup completed
upgrade_platform: Staging the upgrade package -
/var/tmp/junos-srx-mr-vsrx-18.2-2018-2-10.0_RELEASE_182_THROTTLE-linux.tgz..
./
./bzImage-intel-x86-64.bin
./initramfs.cpio.gz
./upgrade_platform
./HOST_COMPAT_VERSION
./version.txt
./initrd.cpio.gz
./linux.checksum
./host-version
bzImage-intel-x86-64.bin: OK
initramfs.cpio.gz: OK
version.txt: OK
upgrade_platform: Checksum verified and OK...
upgrade_platform: Staging of
/var/tmp/junos-srx-mr-vsrx-18.2-2018-2-10.0_RELEASE_182_THROTTLE-linux.tgz
 completed
upgrade_platform: System need *REBOOT* to complete the upgrade
upgrade_platform: Run upgrade_platform with option -r | --rollback to
rollback the upgrade

Host OS upgrade staged. Reboot the system to complete installation!


WARNING:     A REBOOT IS REQUIRED TO LOAD THIS SOFTWARE CORRECTLY. Use the
WARNING:     'request system reboot' command when software installation is
WARNING:    complete. To abort the installation, do not reboot your system,
WARNING:     instead use the 'request system software rollback'
```

```
WARNING:     command as soon as this operation completes.

NOTICE: 'pending' set will be activated at next reboot...
Rebooting. Please wait ...
shutdown: [pid 13050]
Shutdown NOW!

*** FINAL System shutdown message from root@ ***

System going down IMMEDIATELY


Shutdown NOW!

System shutdown time has arrived\x07\x07
```

If no errors occur, Junos OS reboots automatically to complete the upgrade process.

NOTE: Starting in Junos OS Release 17.4R1, upon completion of the vSRX image upgrade the original image will be removed by default as part of the upgrade process.

6. You have successfully upgraded to Junos OS Release 18.2R1 for vSRX. Now log in and use the **show version** command to verify the upgrade.

```
--- JUNOS 18.2-2018-2-10.0_RELEASE_182_THROTTLE Kernel 64-bit
JNPR-11.0-20171012.170745_fbsd-
At least one package installed on this device has limited support.
Run 'file show /etc/notices/unsupported.txt' for details.
root@:~ # cli
root> show version
Model: vsrx
Junos: 18.2-2018-2-10.0_RELEASE_182_THROTTLE
JUNOS OS Kernel 64-bit  [20171012.170745_fbsd-builder_stable_11]
JUNOS OS libs [20171012.170745_fbsd-builder_stable_11]
JUNOS OS runtime [20171012.170745_fbsd-builder_stable_11]
JUNOS OS time zone information [20171012.170745_fbsd-builder_stable_11]
JUNOS OS libs compat32 [20171012.170745_fbsd-builder_stable_11]
JUNOS OS 32-bit compatibility [20171012.170745_fbsd-builder_stable_11]
JUNOS py extensions [20171017.110007_ssd-builder_release_174_throttle]
JUNOS py base [20171017.110007_ssd-builder_release_174_throttle]
JUNOS OS vmguest [20171012.170745_fbsd-builder_stable_11]
JUNOS OS crypto [20171012.170745_fbsd-builder_stable_11]
JUNOS network stack and utilities
[20171017.110007_ssd-builder_release_174_throttle]
JUNOS libs [20171017.110007_ssd-builder_release_174_throttle]
JUNOS libs compat32 [20171017.110007_ssd-builder_release_174_throttle]
JUNOS runtime [20171017.110007_ssd-builder_release_174_throttle]
JUNOS Web Management Platform Package
[20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx libs compat32 [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx runtime [20171017.110007_ssd-builder_release_174_throttle]
JUNOS common platform support
[20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx platform support [20171017.110007_ssd-builder_release_174_throttle]
JUNOS mtx network modules [20171017.110007_ssd-builder_release_174_throttle]
JUNOS modules [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srxtvp modules [20171017.110007_ssd-builder_release_174_throttle]
```

```
JUNOS srxtvp libs [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx libs [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx Data Plane Crypto Support
[20171017.110007_ssd-builder_release_174_throttle]
JUNOS daemons [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx daemons [20171017.110007_ssd-builder_release_174_throttle]
JUNOS Online Documentation [20171017.110007_ssd-builder_release_174_throttle]
JUNOS jail runtime [20171012.170745_fbsd-builder_stable_11]
JUNOS FIPS mode utilities [20171017.110007_ssd-builder_release_174_throttle]
```

Validating the OVA Image

If you have downloaded a vSRX .ova image and need to validate it, see Validating the vSRX .ova File for VMware.

Note that only .ova (VMware platform) vSRX images can be validated. The .qcow2 vSRX images for use with KVM cannot be validated the same way. File checksums for all software images are, however, available on the download page.

System Requirements

System Requirements by Environment

The topics below provide detailed system environment requirement specifications for each supported environment.

- System Requirements for vSRX on AWS
- System Requirements for vSRX on Contrail
- System Requirements for vSRX on KVM
- System Requirements for vSRX on Microsoft Azure
- System Requirements for vSRX on Microsoft Hyper-V
- System Requirements for vSRX on VMware

NOTE: For certain vSRX instance deployments (for example, KVM, VMware, or Contrail), you can scale the performance and capacity of a vSRX instance by increasing the number of vCPUs or the amount of vRAM allocated to the vSRX, but you cannot scale down an existing vSRX instance to a smaller setting.

Hardware Recommendations

Table 2 on page 29 lists the hardware specifications for the host machine that runs the vSRX virtual machine (VM). For additional hardware guidance with respect to a specific software environment, see the *System Requirements* topics listed in the previous section.

Table 2: Hardware Specifications for the Host Machine

Component	Specification
Host memory size	4 GB, 8 GB, 16 GB, or 32 GB. NOTE: Starting in Junos OS Release 15.1X49-D90 and Junos OS Release 17.3R1, the 16-GB host memory size is supported for vSRX on KVM. Starting in Junos OS Release 15.1X49-D100 and Junos OS Release 17.4R1, the 32-GB host memory size is supported for vSRX on KVM.
Host processor type	x86_64 multicore CPU NOTE: DPDK requires Intel Virtualization VT-x/VT-d support in the CPU. See *About Intel Virtualization Technology*.
Physical NIC	• Intel X710/XL710, X520/540, or 82599 physical NICs for SR-IOV on vSRX • Intel XL710 physical NICs for PCI passthrough support on vSRX Starting in Junos OS Release 15.1X49-D70 and Junos OS Release 17.3R1, use Intel 82599 physical NICs in pass-through mode to scale the multicore vSRX. Starting in Junos OS Release 15.1X49-D90 and Junos OS Release 17.3R1, in a KVM deployment you can use SR-IOV (X710/XL710) physical NICs to scale the multicore vSRX. In addition, PCI passthrough (Intel XL710) support is available for vSRX on KVM.

NOTE:

- For VMware, you can check for CPU and other hardware compatibility here: http://www.vmware.com/resources/compatibility/search.php?deviceCategory=cpu
- For KVM, we recommend that you enable hardware-based virtualization on the host machine. You can verify CPU compatibility here: http://www.linux-kvm.org/page/Processor_support

To determine the Junos OS features supported on vSRX, use the Juniper Networks Feature Explorer, a Web-based application that helps you to explore and compare Junos OS feature information to find the right software release and hardware platform for your network. Find Feature Explorer here:

Feature Explorer: vSRX

Best Practices Recommendations

vSRX deployments can be complex, and there is a great deal of variability in the specifics of possible deployments. The following recommendations might apply to and improve performance and function in your particular circumstances.

NUMA Nodes

The x86 server architecture consists of multiple sockets and multiple cores within a socket. Each socket also has memory that is used to store packets during I/O transfers from the NIC to the host. To efficiently read packets from memory, guest applications and associated peripherals (such as the NIC) should reside within a single socket. A penalty is associated with spanning CPU sockets for memory accesses, which might result in nondeterministic performance. For vSRX, we recommend that all vCPUs for the vSRX VM are in the same physical non-uniform memory access (NUMA) node for optimal performance.

CAUTION: The Packet Forwarding Engine (PFE) on the vSRX will become unresponsive if the NUMA nodes topology is configured in the hypervisor to spread the instance's vCPUs across multiple host NUMA nodes. vSRX requires that you ensure that all vCPUs reside on the same NUMA node.

We recommend that you bind the vSRX instance with a specific NUMA node by setting NUMA node affinity. NUMA node affinity constrains the vSRX VM resource scheduling to only the specified NUMA node.

PCI NIC-to-VM Mapping

If the node on which vSRX is running is different from the node to which the Intel PCI NIC is connected, then packets will have to traverse an additional hop in the QPI link, and this will reduce overall throughput. On a Linux host OS, install the **hwloc** package and use the **lstopo** command to provide information about relative physical NIC locations. On a VMware ESX Server, use the **esxtop** command to view information about relative physical NIC locations. On some servers where this information is not available or not supported, refer to the hardware documentation for the slot-to-NUMA node topology.

Mapping Virtual Interfaces to a vSRX VM

To determine which virtual interfaces on your Linux host OS map to a vSRX VM:

1. Use the **virsh list** command on your Linux host OS to list the running VMs.

```
host0S# virsh list
Id    Name                           State
----------------------------------------------------
9     centos1                        running
15    centos2                        running
16    centos3                        running
48    vsrx                           running
50    1117-2                         running
51    1117-3                         running
```

2. Use the **virsh domiflist *vsrx-name*** command to list the virtual interfaces on that vSRX VM.

```
hostOS# virsh domiflist vsrx
Interface  Type       Source     Model       MAC
-------------------------------------------------------
vnet1      bridge     brem2      virtio      52:54:00:8f:75:a5
vnet2      bridge     br1        virtio      52:54:00:12:37:62
vnet3      bridge     brconnect  virtio      52:54:00:b2:cd:f4
```

NOTE: The first virtual interface maps to the fxp0 interface in Junos OS.

Related Documentation

- About Intel Virtualization Technology
- DPDK Release Notes

Finding More Information

For the latest, most complete information about known and resolved issues with the Junos OS, see Juniper Networks Problem Report Search application at:

https://prsearch.juniper.net

Juniper Networks Feature Explorer is a Web-based application that helps you to explore and compare Junos OS feature information to find the correct software release and hardware platform for your network. Find Feature Explorer at:

https://pathfinder.juniper.net/feature-explorer/

Juniper Networks Content Explorer is a Web-based application that helps you explore Juniper Networks technical documentation by product, task, and software release, and download documentation in PDF format. Find Content Explorer at:

https://www.juniper.net/documentation/content-applications/content-explorer/

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback rating system—On any page of the Juniper Networks TechLibrary site at https://www.juniper.net/documentation/index.html, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at https://www.juniper.net/documentation/feedback/.
- E-mail—Send your comments to **techpubs-comments@juniper.net**. Include the document or topic name, URL or page number, and software 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 Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at https://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: https://www.juniper.net/customers/support/
- Search for known bugs: https://prsearch.juniper.net/
- Find product documentation: https://www.juniper.net/documentation/
- Find solutions and answer questions using our Knowledge Base: https://kb.juniper.net/
- Download the latest versions of software and review release notes: https://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: https://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: https://www.juniper.net/cm/

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

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 https://www.juniper.net/cm/.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

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

Revision History

28 June 2018 —Revision 1— Junos OS 18.2R1 – vSRX.