

# Release Notes: Junos<sup>®</sup> OS Release 15.1X49-D160 for the SRX Series

Release 15.1X49-D160  
31 January 2019  
Revision 3

## Contents

Introduction	3
New and Changed Features	4
Release 15.1X49-D160 Software Features	4
AppSecure	4
Routing and Forwarding Options	5
Changes in Behavior and Syntax	6
Interfaces and Routing	6
Known Behavior	6
AppSecure	7
Authentication and Access Control	7
Chassis Cluster	7
Flow-Based and Packet-Based Processing	8
General Packet Radio Service (GPRS)	9
Interfaces and Routing	9
J-Web	9
Layer 2 Ethernet Services	10
Platform and Infrastructure	10
Software Installation and Upgrade	11
Unified Threat Management (UTM)	11
Upgrade and Downgrade	11
User Authentication and Firewall	12
VPNs	12
Known Issues	12
Chassis Cluster	13
Flow-Based and Packet-Based Processing	13
Integrated User Firewall	13
J-Web	13
MPLS	13
Platform and Infrastructure	13
Services Applications	14

Unified Threat Management (UTM) .....	14
VPNs .....	14
Resolved Issues .....	15
Application Layer Gateways (ALGs) .....	15
Chassis Clustering .....	15
CLI .....	16
Flow-Based and Packet-Based Processing .....	16
Interfaces and Routing .....	16
Intrusion Detection and Prevention (IDP) .....	16
J-Web .....	16
Network Address Translation (NAT) .....	17
Platform and Infrastructure .....	17
System Logs .....	17
Unified Threat Management (UTM) .....	17
VPNs .....	17
Documentation Updates .....	18
Migration, Upgrade, and Downgrade Instructions .....	18
Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases .....	18
Product Compatibility .....	19
Hardware Compatibility .....	19
Transceiver Compatibility for SRX Series Devices .....	19
Finding More Information .....	19
Documentation Feedback .....	20
Requesting Technical Support .....	20
Self-Help Online Tools and Resources .....	20
Opening a Case with JTAC .....	21
Revision History .....	21

---

## Introduction

---

Junos OS runs on the following Juniper Networks<sup>®</sup> hardware: ACX Series, EX Series, M Series, MX Series, PTX Series, vSRX, QFabric, QFX Series, SRX Series, and T Series.

These release notes accompany Junos OS Release 15.1X49-D160 for the SRX Series. They describe new and changed features, known behavior, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at <https://www.juniper.net/documentation/software/junos/>.



**NOTE:** Junos OS Release 15.1X49-D160 supports the following devices: SRX300, SRX320, SRX340, SRX345, and High Memory (SRX550M), SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, and SRX5800 devices with host subsystems composed of either an SRX5K-RE-1800X4 (RE2) with an SRX5K-SCBE (SCB2), or an SRX5K-RE-1800X4 (RE2) with an SRX5K-SCB3 (SCB3), and vSRX.

For more details about SRX5400, SRX5600, and SRX5800 devices hardware and software compatibility, please see <https://kb.juniper.net/KB30446>. If you have any questions concerning this notification, please contact the Juniper Networks Technical Assistance Center (JTAC).

---

## New and Changed Features

---

This section describes the new features and enhancements to existing features in Junos OS Release 15.1X49-D160 for the SRX Series devices. For information about new and changed features starting in Junos OS Release 15.1X49-D10 through Junos OS Release 15.1X49-D150, refer to the Release Notes listed in the Release 15.1X49 section at [Junos OS for SRX Series page](#).

- [Release 15.1X49-D160 Software Features on page 4](#)

## Release 15.1X49-D160 Software Features

### AppSecure

---

- **Application-based multipath support (SRX Series and vSRX)**—Starting in Junos OS Release 15.1X49-D160, application-based multipath routing is supported on SRX Series devices.

Multipath identifies two or more paths based on the SLA configuration and triggers a copy of the original traffic on all the identified paths. On the receiving device, while the copy of the packet is in progress, multipath calculates the jitter and packet loss for the combined links and then estimates the jitter and packet loss for the same traffic on individual links. You can compare the reduction in packet loss when combined links are used instead of individual links used for traffic. Sending the multiple copies of the application traffic ensures that if there is a packet loss or delay, the other link might still deliver the packet to the endpoint. Reduction in packet loss, faster delivery of the packet, and less jitter results in better quality of service for the traffic especially for the voice and video traffic.

Multipath support in SD-WAN uses case enhances application experience.

[See [Application Quality of Experience](#).]

- **Application quality of experience scaling support (SRX4100, SRX4200)**—Starting in Junos OS Release 15.1X49-D160, AppQoE enforces configuration limit for overlay paths, metric profiles, probe parameters, and SLA rules per profile when you configure application-specific SLA rules and associate the SLA rules to an APBR profile.

If you configure more parameters than the allowed limit, a warning message is displayed when you commit the configuration.

[See [Application Quality of Experience](#).]

- **AppQoE support in high availability mode (SRX4100, SRX4200)**—Starting in Junos OS Release 15.1X49-D160, AppQoE is supported on SRX4100 and SRX4200 devices when the devices are operating in HA mode.

You can configure the device to operate both in active/active and active/passive modes and deploy the device as spoke device in SD-WAN use cases.

[See [Application Quality of Experience](#).]

- **Application path selection based on link preference and priority (SRX300, SRX320, SRX340, SRX345, SRX550M, SRX1500, SRX4100 SRX4200, and vSRX)**—Starting

in Junos OS Release 18.4R1, you can configure AppQoE to select an application path based on the link priority and the link type when multiple links that meet the SLA requirements are available.

For the application path selection, a list of best paths to a specific destination, which meets the SLA requirements, is made available. From the list, AppQoE selects a path that matches the configured link preference. Paths are the WAN links that are used for forwarding the application traffic. You can select an MPLS or Internet link as the preferred path, and assign a priority. Priority can be any value from the range of values (1-255) with a lower value indicating a more preferred link. A value of one (1) indicates highest priority. If there are multiple paths available, the path that has the highest priority is selected.

[See [Application Quality of Experience](#).]

### Routing and Forwarding Options

- **Virtual routing and forwarding instances (SRX300, SRX320, SRX340, SRX345, SRX550M, SRX1500, SRX4100, SRX4200, and vSRX)**—Starting in Junos OS Release 15.1X49-D160, support is available for MPLS-based configuration on SRX Series devices to deploy them as spoke devices and as hub devices in SD-WAN networks.

As part of MPLS-based implementations, virtual routing and forwarding (VRF) instances are supported in the following modules of an SRX Series device:

- Flow and processing
- Security policy
- NAT
- ALG

The SD-WAN network is segmented based on the Junos VRF routing instances at both spoke and hub locations. VRF instances are required to separate the route of each tenant from other tenants and from other network traffic.

[See [Security Policy for Controlling Traffic for VRF Routing-Instance](#) , [Flow Management in SRX Series Devices Using VRF Routing-Instance](#), [Understanding ALG Support for VRF Routing-Instance](#) , and [Network Address Translation for VRF Routing-Instance](#).]

#### Related Documentation

- [Migration, Upgrade, and Downgrade Instructions on page 18](#)
- [Changes in Behavior and Syntax on page 6](#)
- [Documentation Updates on page 18](#)
- [Known Behavior on page 6](#)
- [Resolved Issues on page 15](#)

## Changes in Behavior and Syntax

---

This section lists the changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands from Junos OS Release 15.1X49-D160.

### Interfaces and Routing

- **Half-duplex link support (SRX340 and SRX345)**—In Junos OS Release 15.1X49-D160, half-duplex mode is supported on SRX340 and SRX345 devices. Half-duplex is bidirectional communication, but signals can flow in only one direction at a time. Full-duplex communication means that both ends of the communication can send and receive signals at the same time. By default, half-duplex is configured. If the link partner is set to autonegotiate the link, then the link is autonegotiated to full duplex or half duplex. If the link is not set to autonegotiation, then the link defaults to half-duplex unless the interface is explicitly configured for full duplex.

#### Related Documentation

- [New and Changed Features on page 4](#)
- [Migration, Upgrade, and Downgrade Instructions on page 18](#)
- [Documentation Updates on page 18](#)
- [Known Behavior on page 6](#)
- [Resolved Issues on page 15](#)

## Known Behavior

---

This section contains the known behaviors, system maximums, and limitations in hardware and software in Junos OS Release 15.1X49-D160.

---

## AppSecure

- On SRX1500 devices, after you change the revocation configuration of a CA profile, the change cannot be populated to the SSL-I revocation check. We recommend that you change the SSL-I configuration to enable or disable the certificate revocation list (CRL) checking instead of the CA profile configuration. [PR1143462](#)

## Authentication and Access Control

- On SRX Series devices, TLS version 1.0 and TLS version 1.1 SSL protocols are blocked because of reported security vulnerabilities. This change might affect users accessing J-Web or the Web authentication GUI, or using dynamic VPN through the Pulse client when using an older Junos OS version or earlier version browsers where TLS version 1.2 protocol is not supported. This change affects Junos OS Release 15.1X49-D100 and later releases. [PR1283812](#)

## Chassis Cluster

- SRX5400, SRX5600, and SRX5800 devices operating in a chassis cluster might encounter the em0 or em1 interface link failure on either of the nodes, which results in split-brain condition. That is, both devices are unable to detect each other. If the failure occurs on the secondary node, the secondary node is moved to the disabled state.

This solution does not cover the following cases:

- em0 or em1 failure on primary node
- HA process restart
- Preempt conditions
- Control link recovery

[PR1363628](#)

- On SRX550M devices in a chassis cluster, traffic loss for about 10 seconds is observed when there is a power failure on the active chassis cluster node. [PR1195025](#)
- On SRX300, SRX320, SRX340, SRX345, and SRX550M devices, if you enable IP monitoring on redundancy groups, the feature might not work correctly on the secondary node if the reth interface has more than one physical interface configured on each node, which enables a redundant Ethernet interface LAG. This issue occurs because the backup node will send traffic using the MAC address of the lowest port in the bundle. If the response towards the same MAC address arrives on a different physical port in the bundle, then the internal switch in the SRX Series device will drop the response packets. [PR1344173](#)

## Flow-Based and Packet-Based Processing

- On SRX5400, SRX5600, and SRX5800 devices, in central point architecture, system logs are sent per second per SPU. Hence, the number of SPUs define the number of system logs per second. [PR1126885](#)
- On SRX1500 devices, the log buffer size is increased to 30,000 in event mode. When the log buffer size is 1000, the Packet Forwarding Engine generates log bursts when there are more than 30 entries and then more logs are dropped. [PR1133757](#)
- On SRX300, SRX320, SRX340, SRX345, and SRX550M devices, the current Ethernet switching MAC aging uses software to age out bulk learned MAC addresses. You cannot age out a specific MAC address learned at a specific time immediately after the configured age. Theoretically, the MAC address might age out close to two times the configured age-out time. [PR1179089](#)
- On SRX300, SRX320, SRX340, SRX345, and SRX550M devices, after a certain period of enabling dot1x, multiple first-message EAP frames with the same timestamp are transmitted. However, this does not affect any dot1x functionality. [PR1245325](#)
- Modem profile is not active until a profile is defined. You need to define a profile before selecting a profile. [PR1254427](#)
- On SRX Series devices, OSPF over GRE over IPsec is not supported on a device with a standalone central point. [PR1274667](#)
- On SRX Series devices, user firewall process useridd retries connecting to the autodiscovery server but fails to connect to the server. Due to this issue, the useridd is unable to handle other messages. Hence, the administrator must remove or deactivate those unused or incorrect user firewall configurations. [PR1307851](#)
- On SRX300, SRX320, SRX340, SRX345, and SRX550M devices, using an SFP-T module can cause an early linkup on connecting a device during the boot process. [PR1314167](#)
- FTP using Microsoft NLB does not work correctly in Layer 2 transparent mode. [PR1341446](#)



## General Packet Radio Service (GPRS)

- During chassis cluster cold synchronization, the GTP-U session is synchronized to the secondary device before the GTP-U tunnel. As a result, the GTP-U tunnel cannot be linked with the corresponding GTP-U flow session. The GTP-U tunnel is not refreshed by the GTP-U traffic until new sessions are created. If an old session does not age out on the primary device, then all the GTP-U traffic goes through fast path and no session creation events are triggered. After the GTP-U timeout period, the tunnels on the secondary device will also age out earlier. [PR1353791](#)

## Interfaces and Routing

- On SRX Series devices, after a user changes some interface configuration, a reboot warning message might appear. The warning message is triggered only when the configuration of the interface mode is changed from route mode to switch or mixed mode. This is a configuration-related warning message and might not reflect the current running state of the interface mode. [PR1165345](#)
- On SRX Series devices, the **show arp** command will show all the ARP entries learned from all interfaces. When Layer 2 global mode is switching, the ARP entries learned from the IRB interface can only show one specific VLAN member port instead of the actual VLAN port learned in the ARP entries. [PR1180949](#)
- On SRX5400, SRX5600, and SRX5800 devices, when CoS is enabled on the st0 interface and the incoming traffic rate destined for the st0 interface is greater than 300,000 packets per second (pps) per SPU, the device might drop some of the high-priority packets internally and shaping of outgoing traffic might be impacted. We recommend that you configure the appropriate policer on the ingress interface to limit the traffic below 300,000 pps per SPU. [PR1239021](#)
- On SRX300, SRX320, SRX340, SRX345, and SRX550M devices, use logical tunnel interface lt-0/0/0 as the destination interface option for an RPM probe server on the device. [PR1257502](#)
- When using a crossover cable, the interfaces are down when there is a change from 10 million to 100 million. [PR1387978](#)

## J-Web

- On SRX550M and SRX1500 devices, there is no option to configure Layer 2 firewall filters from J-Web, irrespective of the device mode. [PR1138333](#)
- On SRX Series devices in a chassis cluster, if you want to use J-Web to configure and commit the configurations, you must ensure that all other user sessions are logged out, including any CLI sessions. Otherwise, the configurations might fail. [PR1140019](#)
- On SRX1500 devices in J-Web, snapshot functionality (Maintain > Snapshot > Target Media > Disk > Click Snap Shot) is not supported. [PR1204587](#)
- On SRX Series devices, DHCP relay configuration under the Configure > Services > DHCP > DHCP Relay page is removed from J-Web in Junos OS Release 15.1X49-D60. The same DHCP relay can be configured using the CLI. [PR1205911](#)

- On SRX Series devices, the DHCP client bindings items under the Monitor menu is removed. The same bindings can be seen in the output of the **show dhcp client binding** CLI command. [PR1205915](#)
- On SRX Series devices, you cannot create profiles for CL-1/0/0 using J-Web and the CLI. An error message, **interface not found**, is displayed. We recommended using only one LTE mPIM in the supported devices. [PR1262543](#)
- On SRX Series devices, when you log in to J-Web and navigate to Monitor>Services>DHCP> DHCP SERVER & DHCP RELAY, click the Help page icon, the Online Help page displays a 404 error message. [PR1267751](#)
- On SRX Series devices, adding 2000 global addresses at a time to the SSL proxy profile exempted addresses can cause the webpage to become unresponsive. [PR1278087](#)
- On SRX Series devices, you cannot view the custom log files created for event logging in J-Web. [PR1280857](#)
- On SRX Series devices, validation is not checked when the UTM policy is detached from the firewall policy rule after an SSL proxy profile is selected. [PR1285543](#)

## Layer 2 Ethernet Services

- On SRX1500 devices configured in Ethernet switching mode, a few MAC entries might still be displayed in the output of the **show ethernet-switching table** command, even after the **age-out** time has passed for all MAC addresses. This issue is applicable only when the MAC learning table entries are equal to or more than 17000 MAC entries. [PR1194667](#)
- On SRX300, SRX320, SRX340, and SRX345 devices, you cannot launch the setup wizard after using the reset configuration button when the device is in Layer 2 transparent mode. You can launch the setup wizard by using the reset configuration button on the device when the device is in switching mode. [PR1206189](#)
- On SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices, VPLS traffic forwarding stops working after enabling the Ethernet switching configuration. VPLS and Ethernet switching must not be configured together on the same device. We recommend not using the Ethernet switching configuration on these devices when VPLS is enabled. [PR1214803](#)
- On SRX Series devices, a packet is not transited by the IRB interface when Layer 2 learning is in switching mode. [PR1218376](#)
- On SRX345 and SRX550M devices, frames carried with a priority bit on Tag Protocol Identifier (TPID) will be lost when the packet passes through with Layer 2 forwarding. [PR1229021](#)

## Platform and Infrastructure

- On SRX5800 devices, if a global SOF policy (all session **service-offload**) is enabled, the connections per second (CPS) will be impacted due to IOC2 limitation. We recommend using an IOC3 card if more sessions are required for SOF or lowering the SOF session amount to make sure the IOC2 is capable of handling it. [PR1121262](#)

- On SRX5800 devices, if the system service REST API is added to the configuration, even though commit can be completed, all the configuration changes in this commit will not take effect. This occurs because the REST API fails to come up and the interface IP address is not available during bootup. The configuration is not read on the Routing Engine side. [PR1123304](#)
- On SRX4100 and SRX4200 devices, although the CLI is configurable, the following features are not supported: Group VPN, VPN Suite B, and encrypted control links when in a chassis cluster. [PR1214410](#)

## Software Installation and Upgrade

- On SRX5000 line devices, in-service software upgrade (ISSU) is not supported when upgrading from earlier Junos OS releases to Junos OS Release 15.1X49. ISSU is supported when upgrading to Junos OS Release 15.1X49 and later.



**NOTE:** SRX300 line devices and SRX550M devices do not support ISSU.

## Unified Threat Management (UTM)

- On SRX Series devices with Sophos Antivirus (SAV) configured, some files that have a size larger than the **max-content-size** might not go into fallback state. Instead, some protocols do not predeclare the content size. [PR1005086](#)
- On SRX Series devices, if AAMW is enabled, and SMTP is configured in the AAMW policy with fallback permission enabled under the long network latency between the devices and AWS is running the Juniper Sky ATP service, there might be a file submission timeout error. When sending the timeout error, there is a possibility that the e-mail sent from Outlook might stay in the outbox of the sender, and the receiver might not receive the e-mail. [PR1254088](#)
- On SRX Series devices, AAMW established sessions always use the configured AAMW parameters at the time of session establishment. The configuration changes will not retroactively affect the already established sessions. For example, a session established when the verdict threshold is 5 will always have 5 as the threshold even if the verdict threshold changes to other values during the session lifetime. [PR1270751](#)

## Upgrade and Downgrade

- When you perform a firmware upgrade or downgrade, a FIPS core file is generated. In Junos OS FIPS mode, the file integrity checking application **verifexec** treats the new updated firmware file as a corrupted Junos OS file. This is an expected behavior by design. [PR1268240](#)
- After you upgrade from Junos OS Release 15.1X49-D40 to Junos OS Release 15.1X49-D120, node0 was stuck at the grub loader stage. [PR1347046](#)

## User Authentication and Firewall

- On SRX Series devices, firewall authentication cannot retrieve domain information from the access profile configuration. That is because the firewall authentication will not push user domain information to the Juniper Identity Management Service server in case the user authenticates through **web-authentication**, **pass-through**, or **web-redirect** with an LDAP access profile. [PR1281063](#)
- Primary group-domain computers are not supported by the user firewall integration. [PR1361512](#)

## VPNs

- On SRX Series devices, if an IPsec VPN tunnel is established using IKEv2 because of bad SPI, packet drop might be observed during **CHILD\_SA rekey** when the device is the responder for this rekey. [PR1129903](#)
- On SRX1500 devices in a chassis cluster with the Juniper Sky ATP solution deployed, if you disable and then reenables CRL checking of certificate validity, the system does not reenables CRL checking. [PR1144280](#)
- On SRX5400, SRX5600, and SRX5800 devices, when CoS is enabled on the st0 interface and the incoming traffic rate destined for the st0 interface is higher than 300,000 packets per second (pps) per SPU, the device might drop some of the high-priority packets internally and shaping of outgoing traffic may be impacted. We recommended that you configure the appropriate policer on the ingress interface to limit the traffic below 300,000 pps per SPU. [PR1239021](#)

### Related Documentation

- [New and Changed Features on page 4](#)
- [Migration, Upgrade, and Downgrade Instructions on page 18](#)
- [Changes in Behavior and Syntax on page 6](#)
- [Known Behavior on page 6](#)
- [Resolved Issues on page 15](#)

## Known Issues

---

This section lists the known issues in hardware and software in Junos OS Release 15.1X49-D160.

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

## Chassis Cluster

- On SRX Series devices, the flowd process might stop during an ISSU in a rare racing condition. [PR1386522](#)

## Flow-Based and Packet-Based Processing

- On SRX Series devices, OSPF over GRE over IPsec is not supported on a device with a standalone central point. [PR1274667](#)
- On SRX Series devices with chassis cluster enabled in active/active mode, when the multicast traffic crosses multiple logical systems (LSYS) and also crosses the fabric link (Z-mode traffic), some sessions might not be cleared after aging out. [PR1295893](#)

## Integrated User Firewall

- On SRX Series devices running integrated user firewall, group membership changes are not processed correctly after a user's Windows logon account name is modified while retaining the same distinguished name. [PR1394049](#)

## J-Web

- On SRX Series devices, if the configuration load is more than 5000 bytes, then J-Web responds slowly and the navigation of pages might take more time. [PR1222010](#)
- On SRX4100 devices, a security policy page in J-Web does not load when it has 40,000 firewall policies configured. Navigate to the Configure > Security > Security Policy page. [PR1251714](#)
- On SRX Series devices, the dashboard widget applications, ThreatMap, and Firewall Top Denies indicate that no data is available even when the device has a large amount of data. [PR1282666](#)
- On SRX Series devices, the CLI terminal does not work for Google Chrome version later than version 42. You can use Internet Explorer 10 or 11 or Mozilla Firefox 46 browsers to use the CLI terminal. [PR1283216](#)

## MPLS

- On SRX550M devices in a chassis cluster, the BGP and OSPF flapped causing traffic loss and the rpd process to stop. [PR1366575](#)

## Platform and Infrastructure

- On SRX Series devices running FreeBSD 6-based Junos OS, the system might panic when a USB flash drive with a mounted file system is physically detached by a user. [PR695780](#)
- On SRX5800 devices, even though the system service REST API is configured and committed, all the configuration changes in this commit do not take effect. This issue occurs because the REST API process fails to come up and the interface IP address is

not available during startup. The configuration is not read by the Routing Engine.

[PR1123304](#)

- On SRX Series devices, the flowd process might stop and cause traffic outage if the SPU CPU usage is higher than 80 percent. Therefore, some threads are in waiting status and the watchdog cannot be toggled timely, causing the flowd process to stop. [PR1162221](#)
- On SRX Series devices, mgd core files are generated during RPC communication between the SRX Series device and Junos Space or Junos OS CLI with the percent sign (%) present in the RPC description or annotation. [PR1287239](#)
- On SRX5600 and SRX5800 devices in a chassis cluster, when a second Routing Engine is installed to enable dual control links, the **show chassis hardware** operational command might show the same serial number for both the second Routing Engines on both the nodes. [PR1321502](#)
- If failover occurs while the device is handling many concurrent Web authentication requests, the CPU usage of the httpd process might be high. [PR1352133](#)
- When a device failover occurs while handling concurrent Web authentication requests, the httpd might work incorrectly because the program PHP cannot exit properly. Therefore, the system creates a new httpd process to handle the new Web authentication requests. [PR1352894](#)

## Services Applications

- If J-Flow version 9 is configured on the device, the flowd process might stop, causing traffic loss. [PR1370389](#)

## Unified Threat Management (UTM)

- On SRX Series devices, the log collector does display the zone information. [PR1326271](#)

## VPNs

- On SRX Series devices, if an IPsec VPN tunnel is established using IKEv2 because of an incorrect security parameter index (SPI), packet drop might be observed during a CHILD\_SA rekey when the device is the responder for this rekey. [PR1129903](#)
- On SRX1500 devices in a chassis cluster with the Juniper Sky ATP solution deployed, if you disable and then reenables the CRL checking of certificate validity, the system does not reenables the CRL checking. [PR1144280](#)
- On SRX Series devices, if multiple traffic selectors are configured for a peer with IKEv2 reauthentication, only one traffic selector will rekey at the time of IKEv2 reauthentication. The VPN tunnels of the remaining traffic selectors are cleared without immediate rekeying. New negotiation of those traffic selectors might trigger through other mechanisms such as traffic or by peer. [PR1287168](#)

- The VPN tunnels in two chassis cluster nodes can be out-of-synchronization after the VPN generates a core file in the active chassis cluster node. The out-of-synchronization VPN tunnels can impact traffic. [PR1351646](#)
- On SRX Series devices, when GCM is used as an encryption algorithm, the kmd process might stop when the SNMP polls for the IKE SA on the device. [PR1397897](#)

#### Related Documentation

- [New and Changed Features on page 4](#)
- [Migration, Upgrade, and Downgrade Instructions on page 18](#)
- [Changes in Behavior and Syntax on page 6](#)
- [Documentation Updates on page 18](#)
- [Resolved Issues on page 15](#)

## Resolved Issues

This section lists the issues fixed in hardware and software in Junos OS Release 15.1X49-D160. For information about resolved issues in Junos OS Release 15.1X49-D10 through Junos OS Release 15.1X49-D150, refer to the Release Notes listed in the Release 15.1X49 section at [Junos OS for SRX Series page](#).

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

### Application Layer Gateways (ALGs)

- DNS requests with EDNS option might be dropped by the DNS ALG. [PR1379433](#)
- Sun RPC data traffic for previously established ALG sessions might be dropped because it matches the gate, which contains old interface information. [PR1387895](#)
- The flowd process might generate core files while sending cross-tenant ALG traffic. [PR1388658](#)

### Chassis Clustering

- On SRX340 and SRX345 devices, half-duplex mode is not supported. [PR1149904](#)
- On SRX550M device, the SFP transceiver does not work after the chassis reboot. [PR1347874](#)
- The device in chassis cluster mode might be unresponsive if IP monitoring is enabled. [PR1366958](#)
- Multiple flowd process files are seen on node 1 after an RGO failover. [PR1372761](#)
- Traffic loss occurs when the primary node is rebooting. [PR1372862](#)
- The SNMP trap was sending incorrect information. [PR1378903](#)

- On SRX Series devices in a chassis cluster, if reroute occurs on the IPv4 wings of a NAT64 or NAT46 session, the active node will send RTO message to the backup session to update the rerouted interface. [PR1379305](#)
- On SRX Series devices, the MIB OID **dot3StatsDuplexStatus** always shows full duplex. [PR1383120](#)

## CLI

- The following CLI command outputs are not displayed correctly: **show usp memory segment shm data module** and **show jsf shm module**. [PR1387711](#)

## Flow-Based and Packet-Based Processing

- SRX1500 fan speed often fluctuates. [PR1271024](#)
- The fan speed might frequently keep changing between normal and full. [PR1316192](#)
- The mgd process might stop after invoking a specific RPC; the SSH or the console need to be reconnected. [PR1335523](#)
- The VPLS connection fails after a node reboot. [PR1350587](#)
- On SRX1500 devices, the **Fan Tray 0 Fan 0 Spinning Degraded** alarm is displayed. [PR1367334](#)
- On SRX Series devices, the PIM register message might be dropped. [PR1378295](#)
- The device does not send messages **frag needed** and **DF set** back to the source host during path MTU discovery. [PR1389428](#)

## Interfaces and Routing

- On SRX1500 devices, IPv4 multicast packets cannot be broadcasted from the IRB interface. [PR1385934](#)

## Intrusion Detection and Prevention (IDP)

- IDP cannot be deployed, because the IDP configuration is unable to commit. [PR1374079](#)

## J-Web

- When you change the application firewall **rule-set** action from J-Web, the default rule action changes unintentionally. [PR1379042](#)
- The chassis image did not display on the J-Web dashboard. [PR1382219](#)
- The J-Web displays that the CPU is overheating. [PR1389981](#)



---

## Network Address Translation (NAT)

- Source NAT sessions might fail to be created when **port-overloading** or the **port-overloading-factor** is configured. [PR1370279](#)

## Platform and Infrastructure

- Packet capture feature does not work after removing the sampling configuration. [PR1370779](#)
- On SRX Series devices in a chassis cluster, the cold synchronization process might slow down when there are many Packet Forwarding Engines installed on the device. [PR1376172](#)
- The **uspic failed** messages appear while running the **show interface extensive** command from the CLI. [PR1380439](#)
- Junos OS upgrade might fail with the **validate** option after the **/cf/var/sw** directory is erroneously deleted. [PR1384319](#)

## System Logs

- A warning syslog message is displayed when the number of security screens installed exceeds the IOC capacity. [PR1209565](#)
- On SRX Series devices, false log messages are observed: **/kernel: check\_configured\_tpid: <interface> : default tpid (0x8100) not configured. pic allows maximum of 0 tpid.** [PR1373668](#)

## Unified Threat Management (UTM)

- The enhanced Web filtering server status shows "UP" when 443 is specified as the server port. [PR1336235](#)

## VPNs

- On SRX1500 devices, the kmd process might stop when configuring IPsec VPN and BGP. [PR1351727](#)
- If the certificate authority (CA) profile name has a period (.), the PKI daemon (process) encounters issues if it is restarted. [PR1351727](#)
- VPN tunnels might not be configured successfully and the VPN tunnels might not come up. [PR1376134](#)
- Packet loss is observed in IPsec Z-mode scenario. [PR1377266](#)
- The kmd process might stop and cause VPN traffic outage after running the **show security ipsec next-hop-tunnels** command. [PR1381868](#)
- Adding or deleting site-to-site manual NHTB VPN tunnels to an existing st0 unit causes the existing manual NHTB VPN tunnels under the same st0 unit to flap. [PR1382694](#)

- Related Documentation**
- [New and Changed Features on page 4](#)
  - [Migration, Upgrade, and Downgrade Instructions on page 18](#)
  - [Changes in Behavior and Syntax on page 6](#)
  - [Known Behavior on page 6](#)
  - [Known Behavior on page 6](#)

---

## Documentation Updates

There are no errata or changes in Junos OS Release 15.1X49-D160 for the SRX Series documentation.

---

## Migration, Upgrade, and Downgrade Instructions

This section contains the procedure to upgrade Junos OS, and the upgrade and downgrade policies for Junos OS. Upgrading or downgrading Junos OS can take several hours, depending on the size and configuration of the network.

- [Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases on page 18](#)

### Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases

Support for upgrades and downgrades that span more than three Junos OS releases at a time is not provided, except for releases that are designated as Extended End-of-Life (EEOL) releases. EEOL releases provide direct upgrade and downgrade paths—you can upgrade directly from one EEOL release to the next EEOL release even though EEOL releases generally occur in increments beyond three releases.

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 12.3X48, 15.1X49, 17.3, and 17.4 are EEOL releases. You can upgrade from Junos OS Release 15.1X49 to Release 17.3 or from Junos OS Release 15.1X49 to Release 17.4. However, you cannot upgrade directly from a non-EEOL release that is more than three releases ahead or behind.

Upgrade from Junos OS Release 17.4 to successive Junos OS Release, is supported. However, you cannot upgrade directly from a non-EEOL release that is more than three releases ahead or behind.

To upgrade or downgrade from a non-EEOL release to a release more than three releases before or after, first upgrade to the next EEOL release and then upgrade or downgrade from that EEOL release to your target release.

For more information about EEOL releases and to review a list of EEOL releases, see <https://www.juniper.net/support/eol/junos.html>.

For information about software installation and upgrade, see the [Installation and Upgrade Guide for Security Devices](#).

For information about ISSU, see the [Chassis Cluster Feature Guide for Security Devices](#).

#### Related Documentation

- [New and Changed Features on page 4](#)
- [Changes in Behavior and Syntax on page 6](#)
- [Documentation Updates on page 18](#)
- [Known Behavior on page 6](#)
- [Resolved Issues on page 15](#)

## Product Compatibility

---

This section lists the product compatibility for any Junos OS SRX Series mainline or maintenance release.

- [Hardware Compatibility on page 19](#)
- [Transceiver Compatibility for SRX Series Devices on page 19](#)

### Hardware Compatibility

To obtain information about the components that are supported on the device, and special compatibility guidelines with the release, see the SRX Series Hardware Guide.

To determine the features supported on SRX Series devices in this release, 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 at <https://pathfinder.juniper.net/feature-explorer/>.

### Transceiver Compatibility for SRX Series Devices

We strongly recommend that only transceivers provided by Juniper Networks be used on SRX Series interface modules. Different transceiver types (long-range, short-range, copper, and others) can be used together on multiport SFP interface modules as long as they are provided by Juniper Networks. We cannot guarantee that the interface module will operate correctly if third-party transceivers are used.

Please contact Juniper Networks for the correct transceiver part number for your device.

## Finding More Information

---

For the latest, most complete information about known and resolved issues with the Junos OS, see the Juniper Networks Problem Report Search application at <https://prsearch.juniper.net>.

For regulatory compliance information about [Common Criteria](#), [FIPS](#), [Homologation](#), [RoHS2](#), and [USGv6](#) for Juniper Networks products, see the [Juniper Networks Compliance Advisor](#).

To access Software Release Notifications for Junos OS Service Releases, visit our Knowledge Center at <https://support.juniper.net/support/>. You'll need to log in to your Juniper Account. From the Knowledge Center, search by the specific release number, for example 17.4R1-S2. Use the Software Release Notifications to download software, and learn about known and resolved issues for specific service releases.

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://apps.juniper.net/feature-explorer/>.

## 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](mailto:techpubs-comments@juniper.net), or fill out the documentation feedback form at <https://www.juniper.net/cgi-bin/docbugreport/>. If you are using e-mail, be sure to include the following information with your comments:

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

## Requesting Technical Support

---

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

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 <https://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://support.juniper.net/support/>
- Search for known bugs: <https://kb.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://support.juniper.net/support/downloads/>
- Search technical bulletins for relevant hardware and software notifications: <https://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <https://forums.juniper.net>
- 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, visit us at <https://support.juniper.net/support/requesting-support/>.

If you are reporting a hardware or software problem, issue the following command from the CLI before contacting support:

```
user@host> request support information | save filename
```

To provide a core file to Juniper Networks for analysis, compress the file with the **gzip** utility, rename the file to include your company name, and copy it to **ftp.juniper.net/pub/incoming**. Then send the filename, along with software version information (the output of the **show version** command) and the configuration, to **support@juniper.net**. For documentation issues, fill out the bug report form located at <https://www.juniper.net/documentation/feedback/>.

## Revision History

31, January 2019—Revision 3— Junos OS 15.1X49-D160 – SRX Series.

28, January 2019—Revision 2— Junos OS 15.1X49-D160 – SRX Series.

20, December 2018—Revision 1— Junos OS 15.1X49-D160 – SRX Series.

Copyright © 2019 Juniper Networks, Inc. All rights reserved.

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. and/or its affiliates in the United States and other countries. All other trademarks may be property of their respective owners.

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