

# Release Notes: Junos<sup>®</sup> OS Release 15.1X49-D220 for the SRX Series

Release 15.1X49-D220  
7 July 2020  
Revision 2

<b>Contents</b>	<b>Introduction   3</b>
	<b>New and Changed Features   4</b>
	Release 15.1X49-D220 Software Features   4
	<b>Changes in Behavior and Syntax   4</b>
	<b>Known Limitations   5</b>
	Authentication and Access Control   5
	Chassis Clustering   6
	Flow-Based and Packet-Based Processing   6
	Interfaces and Chassis   8
	J-Web   8
	Platform and Infrastructure   9
	Unified Threat Management (UTM)   10
	VPNs   10
	<b>Open Issues   11</b>
	Flow-Based and Packet-Based Processing   11
	Install and Upgrade   12
	Interfaces and Chassis   12
	J-Web   13
	Network Management and Monitoring   14
	Platform and Infrastructure   14
	Routing Policy and Firewall Filters   15
	VPNs   15

**Resolved Issues | 16****Application Layer Gateways (ALGs) | 16****Flow-Based and Packet-Based Processing | 16****Routing Policy and Firewall Filters | 17****Unified Threat Management (UTM) | 17****Documentation Updates | 17****Chassis Clustering | 17****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 | 20****Finding More Information | 20****Documentation Feedback | 20****Requesting Technical Support | 21****Self-Help Online Tools and Resources | 22****Opening a Case with JTAC | 22****Revision History | 23**

# Introduction

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

These release notes accompany Junos OS Release 15.1X49-D220 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-D220 supports the following devices: SRX300, SRX320, SRX340, SRX345, SRX550M (High Memory), 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, see <https://kb.juniper.net/InfoCenter/index?page=content=KB21476>. If you have any questions concerning this notification, please contact the Juniper Networks Technical Assistance Center (JTAC).

# New and Changed Features

## IN THIS SECTION

- [Release 15.1X49-D220 Software Features | 4](#)

This section describes new features and enhancements to existing features in Junos OS Release 15.1X49-D220 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-D210, see the Release Notes listed in the Release 15.1X49 section at [Junos OS for SRX Series page](#).

## Release 15.1X49-D220 Software Features

There are no new features in Junos OS Release 15.1X49-D220 for the SRX Series devices.

### RELATED DOCUMENTATION

<a href="#">Changes in Behavior and Syntax   4</a>
<a href="#">Known Limitations   5</a>
<a href="#">Open Issues   11</a>
<a href="#">Resolved Issues   16</a>
<a href="#">Documentation Updates   17</a>

## Changes in Behavior and Syntax

Junos OS Release 15.1X49-D220 does not have any changes in behavior and syntax for SRX Series devices.

### RELATED DOCUMENTATION

<a href="#">New and Changed Features   4</a>
--

Known Limitations   5
Open Issues   11
Resolved Issues   16
Documentation Updates   17

## Known Limitations

### IN THIS SECTION

- Authentication and Access Control | 5
- Chassis Clustering | 6
- Flow-Based and Packet-Based Processing | 6
- Interfaces and Chassis | 8
- J-Web | 8
- Platform and Infrastructure | 9
- Unified Threat Management (UTM) | 10
- VPNs | 10

This section contains the known behaviors, system maximums, and limitations in hardware and software in Junos OS Release 15.1X49-D220.

### 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 version of Junos OS or older versions of browsers that do not support the TLS version 1.2 protocol. This change affects Junos OS Release 15.1X49-D100 and later releases. [PR1283812](#)
- On SRX4100, SRX4200, SRX4600, vSRX, and SPC3 platforms, bandwidth policers might cause low throughput when processing high-rate multiflow traffic. [PR1459936](#)

## Chassis Clustering

- In a chassis cluster setup on SRX550M devices, traffic loss for about 10 seconds is observed when there is a power failure on the active chassis cluster node. [PR1195025](#)
- IP monitoring for redundancy groups might not work on the secondary node if the reth interface has more than one physical interfaces configured. This is because the backup node sends traffic using the MAC address of the lowest port in the bundle. If the reply does not come back on the same physical port, then the internal switch drops the traffic. [PR1344173](#)
- During chassis cluster cold synchronization, the GTP-U session is synchronized with the secondary device before it is synchronized with the GTP-U tunnel. As a result, the GTP-U tunnel cannot be linked with the corresponding GTP-U flow session, and the GTP-U tunnel is not refreshed by GTP-U traffic until new sessions are created. If old sessions do not age out on the primary device, all GTP-U traffic goes through fast path and no session creation events are triggered. Then, after the GTP-U timeout period, the tunnels on the secondary device also age out earlier. [PR1353791](#)

## Flow-Based and Packet-Based Processing

- On SRX Series devices, the **show arp** command displays all the ARP entries learned from all interfaces. While switching to Layer 2 global mode, the ARP entries learned from the IRB interface show only one specific VLAN member port instead of the actual VLAN port learned in the ARP entries. [PR1180949](#)
- 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 occurs only when the MAC learning table has 17,000 MAC entries or more. [PR1194667](#)
- On SRX300, SRX320, SRX340, and SRX345 devices, you cannot launch the setup wizard by 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 only when the device is in switching mode. [PR1206189](#)
- On SRX300, SRX320, SRX340, SRX345, and SRX1500 devices, the vSRX 2.0 command **set system internet-options tcp-mss** does not work in Junos OS Release 15.1X49. [PR1213775](#)
- On SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices, VPLS and Ethernet switching must not be configured together on the same device. We recommend that you avoid using an Ethernet-switching configuration on these platforms when VPLS is enabled. [PR1214803](#)
- On SRX345 and SRX550M devices, frames carried with a priority bit on the Tag Protocol Identifier (TPID) are lost when the packet passes through with Layer 2 forwarding. [PR1229021](#)

- On SRX300, SRX320, SRX340, SRX345, and SRX550M devices, after a certain period of enabling 802.1X, multiple first-message EAP frames with the same timestamp are transmitted. This does not affect any 802.1X functionality. [PR1245325](#)
- On SRX Series devices, if the advanced anti-malware (AAMW) service is enabled, 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, then the file submission timeout error might occur. When sending the timeout error, the e-mail sent from Outlook might remain in the outbox of the sender, and the recipient might not receive the e-mail. [PR1254088](#)
- A modem profile is not active until the profile is defined. You need to define a profile before selecting it. [PR1254427](#)
- A FIPS core file is generated when you perform a firmware upgrade or downgrade. In Junos OS FIPS mode, the file integrity checking application veriexec treats the new updated firmware file as a corrupted Junos OS file. [PR1268240](#)
- On SRX Series devices, established AAMW sessions always use the configured AAMW parameters that exist at the time of session establishment. Configuration changes do not retroactively affect the already established sessions. For example, a session established when the verdict threshold is 5 always has 5 as the threshold even if the verdict threshold changes to other values during the session lifetime. [PR1270751](#)
- On SRX Series devices, OSPF over GRE running on IPsec is not supported on a device with a standalone central point. [PR1274667](#)
- On SRX Series devices, firewall authentication cannot retrieve domain information from the access profile configuration because firewall authentication does not push user domain information to the Juniper Identity Management Service server if the user authenticates through Web authentication, pass-through, or Web redirect with an LDAP access profile. [PR1281063](#)
- The user firewall process useridd repeatedly attempts to reconnect to the AD server when the connection fails. Consequently, useridd is unable to handle other messages. You (the administrator) must remove or deactivate 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 if you connect a device during the boot process. [PR1314167](#)
- Packet reordering occurs on the traffic received on the PPP interface. [PR1340417](#)
- FTP using Microsoft NLB does not work correctly in transparent mode. [PR1341446](#)
- Primary group-domain computers are not supported by the user firewall integration. [PR1361512](#)
- When using a crossover cable, the interfaces are down when there is a change from 10 million to 100 million. [PR1387978](#)
- When using advanced, application-based, multipath routing, the sender sequences packets in order and delivers the packets to the receiver. If the receiver receives the packets out of order, then in Junos OS Release 15.1X49-D200 and later, the packets are dropped. Because IPsec might reorder packets coming from the sender for fragmentation, packets might get dropped at the receiver. [PR1403584](#)

- Packets might be dropped in an SD-WAN use case if IPsec is not configured (for example, IP over MPLS over GRE) in HA Z mode. This issue does not occur if IPsec is configured (IP over MPLS over GRE over IPsec) or in chassis cluster active/passive mode. [PR1415343](#)
- On all SRX Series devices, when a flow containing fragmented IP packets passes through the firewall of an SRX Series device, if the same IP ID value is used by two different fragmented packets within 2 seconds, the second fragmented IP packet is dropped. [PR1482074](#)

## Interfaces and Chassis

- On SRX Series devices, after the user changes some interface configurations, 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, so it might not reflect the current running state of the interface mode. [PR1165345](#)
- On SRX300, SRX320, SRX340, SRX345, and SRX550M devices, the current Ethernet switching MAC aging uses software to age out MAC addresses learned in bulk. You cannot age out a specific MAC address learned at a specific time immediately after the configured age. The MAC address might age out close to two times the configured age-out time. [PR1179089](#)
- On SRX300, SRX320, SRX340, SRX345, and SRX550M devices, use the logical tunnel interface lt-0/0/0 as the destination interface option for an RPM probe server on the device. [PR1257502](#)

## 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 configurations, you must ensure that all other user sessions are logged out, including any CLI sessions. Otherwise, the configurations might fail. [PR1140019](#)
- On SRX Series devices, adding 2000 global addresses at a time to the addresses exempted in the SSL proxy profile can cause the webpage to become unresponsive. [PR1278087](#)
- On SRX1500 devices in J-Web, the snapshot functionality Maintain>Snapshot>Target Media>Disk>Click Snap Shot is not supported. [PR1204587](#)
- On SRX Series devices, you cannot create profiles for CL-1/0/0 using J-Web and the CLI. The error message **interface not found** is displayed. We recommend that you use only one LTE Mini-PIM in the supported devices. [PR1262543](#)



- On SRX Series devices, when you log in to J-Web, navigate to Monitor>Services>DHCP>DHCP Relay, and click the Help page icon, the Online Help page displays a 404 error message. [PR1267751](#)
- On SRX Series devices, you cannot view the custom log files created for event logging in J-Web. [PR1280857](#)
- On SRX Series devices running Junos OS Release 15.1X49-D90 and earlier releases, J-Web often does not display the IPD log that is locally saved. [PR1336341](#)
- On SRX Series devices using Junos OS Release 15.1X49, a J-Web operation does not reset the idle time in the output of the **show system users** command. [PR1445779](#)

## Platform and Infrastructure

- On SRX5800 devices, if a global SOF policy (all session service-offload) is enabled, the connections per second are impacted due to an IOC2 limitation. We recommend that you use an IOC3 card if more sessions are required for SOF, or lower the SOF session amount to ensure that IOC2 is capable of handling it. [PR1121262](#)
- On SRX5800 devices, if the system service REST API is added to the configuration, even though the commit can be completed, all the configuration changes in this commit do not take effect. This occurs because the REST API daemon 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 SRX5400, SRX5600, and SRX5800 devices, in a 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 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 chassis cluster. [PR1214410](#)
- On SRX1500 devices, when a 1-Gigabit Ethernet SFP-T transceiver is used on 1-Gigabit Ethernet SFP ports (ge-0/0/12 through ge-0/0/15), the ge interface does not operate at 100-Mbps speed. [PR1133384](#)
- On all SRX Series devices, when you are using event mode logging, some AppTrack log messages might be lost in case of heavy logging. The reason is that the Packet Forwarding Engine might send the messages in batches, overflowing the log buffer on the Routing Engine. The log buffer has been increased as a mitigation, but in rare instances, some log messages might still be dropped. [PR1133757](#)
- On SRX1500 devices, when CPU usage is very high (above 95 percent), the connection between the AAMW process and PKI daemon might break. In this case, the AAMW process remains in initializing state until that connection is established. [PR1142380](#)
- 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 certificate revocation list (CRL) checking instead of CA profile configuration. [PR1143462](#)

- On SRX1500 devices in a chassis cluster with the Juniper Sky Advanced Threat Prevention (ATP) solution deployed, if you disable and then reenables CRL checking of certificate validity, the system does not reenables CRL checking. [PR1144280](#)
- On SRX340 and SRX345 devices, half-duplex mode is not supported. [PR1149904](#)
- On SRX5400 devices, if a username or group name contains the characters \* (ASCII 0x2a), (ASCII 0x28), (ASCII 0x29), \ (ASCII 0x5c), and NUL (ASCII 0x00), the query from the device to the LDAP server times out and might lead to high CPU utilization. [PR1157073](#)
- On SRX300 and SRX320 devices, link mode cannot be set to half-duplex mode on internal small form-factor pluggable (SFP) ports. [PR1165259](#)
- When using a third-party certificate chain for the Web authentication redirect page, for the HTTP REST API, or for J-Web access, which contains at least one intermediate CA certificate, the SRX Series device does not send the intermediate certificate to the client. [PR1408921](#)
- SRX320 PoE devices do not support LLDP from Junos OS Release 15.1X49-D170 onward. [PR1438467](#)

## Unified Threat Management (UTM)

- On SRX Series devices with Sophos Antivirus (SAV) configured, some files that have size larger than the **max-content-size** might not go into fallback state. This might occur when a protocol does not predeclare the content size. [PR1005086](#)
- On SRX550M devices using Junos OS Release 12.1X49-D30 for the enhanced Web filtering feature, performance drop is observed. [PR1138189](#)

## VPNs

- On SRX Series devices, an IPsec VPN tunnel that uses a PPPoE interface as the external interface fails after RGO failover. [PR1143955](#)
- 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 might be impacted. We recommend that you configure an appropriate policer on the ingress interface to limit the traffic to below 300,000 pps per SPU. [PR1239021](#)

## RELATED DOCUMENTATION

New and Changed Features   4
Changes in Behavior and Syntax   4
Open Issues   11
Resolved Issues   16
Documentation Updates   17

## Open Issues

### IN THIS SECTION

- Flow-Based and Packet-Based Processing | 11
- Install and Upgrade | 12
- Interfaces and Chassis | 12
- J-Web | 13
- Network Management and Monitoring | 14
- Platform and Infrastructure | 14
- Routing Policy and Firewall Filters | 15
- VPNs | 15

This section lists the known issues in hardware and software in Junos OS Release 15.1X49-D220.

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

### Flow-Based and Packet-Based Processing

- On SRX550M devices, upgrade fails when you upgrade from Junos OS Release 15.1X49-D30 to a later release without using the **no-validate** option. [PR1237971](#)
- On SRX Series devices, if the advanced anti-malware (AAMW) service is enabled, 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, file submission timeout error might occur.

When sending the timeout error, the e-mail sent from Outlook might remain in the outbox of the sender, and the recipient might not receive the e-mail. [PR1254088](#)

- SNMP fails while polling data across custom routing instances on the SRX300 line of devices. [PR1352311](#)
- On all SRX Series devices, in a chassis cluster with Z-mode traffic and local (non-reth) interfaces configured, when using ECMP routing between multiple interfaces residing on both node0 and node1, if a session is initiated through one node and the return traffic comes in through the other node, packets might be dropped due to reroute failure. [PR1410233](#)
- On all SRX Series devices with the advanced anti-malware service configured, due to a rare issue in file system handling in the data plane, the flowd or srpxfe process might stop. [PR1437270](#)
- On SRX1500 devices, the link does not come up after you replace a copper transceiver with a fiber transceiver until you reboot the device. [PR1437615](#)
- An unexpected IP address is included in the custom IP feed on an SRX4100 cluster. You can resolve this issue by restarting the security intelligence process. [PR1440157](#)
- The TCP session cannot time out properly upon receiving the TCP RESET packet, and the session timeout value does not change to 2 seconds. [PR1467654](#)

## Install and Upgrade

- On SRX1500 devices in a chassis cluster with the Juniper Sky Advanced Threat Prevention (ATP) solution deployed, if you disable and then reenale CRL checking of certificate validity, the system does not reenale CRL checking. [PR1144280](#)

## Interfaces and Chassis

- On SRX300, SRX320, SRX340, SRX345, and SRX550M devices, for logical interface scaling without **per-unit-scheduler** configured, the total number of logical interfaces is limited to 2048. With **per-unit-scheduler** configured on the physical interface, the total number of logical interfaces is limited to the CoS scheduler subunit upper limit of 2048. So, the maximum number of logical interfaces for **per-unit-scheduler** should be 2048 minus the number of physical interfaces that are up. With at least one logical interface up, the maximum number is 128. [PR1138997](#)
- The **monitor interface** command starts the ifmon process. During this time, if the Telnet session to the router is disconnected unconventionally, then the ifmon process is not terminated and takes up 100 percent CPU utilization. The workaround is to terminate the stale ifmon process. [PR1162521](#)
- On the SRX4000 line of devices, the fxp0 interface status does not show the proper state for speed and duplex. [PR1392050](#)

- The multipath credit limit might be reset after multiple configuration changes and interface flaps. The credit limit might be reset based on the default interface speed of 1 Gbps and the default or configured bandwidth limit. [PR1401090](#)
- T1 interfaces go down if Password Authentication Protocol (PAP) RADIUS authentication is configured. [PR1402612](#)
- On SRX1500 platforms, if you configure **interface-mac-limit** on one interface and then send traffic with a different source MAC address (such as 10,000) on that interface, then the number of learned MAC addresses reaches the maximum limit (8192). Traffic cannot be transferred on all interfaces. [PR1409018](#)

## J-Web

- On SRX4100 devices, a security policy page in J-Web does not load when it has 40,000 firewall policy configurations. Navigate to the Configure> Security> Security Policy page. [PR1251714](#)
- On SRX Series devices, the dashboard widget applications, ThreatMap, and Firewall Top Denies initially show no data available even when the device has a large amount of data. Refresh the individual widgets to show the data. [PR1282666](#)
- On SRX Series devices, the CLI terminal does not work for Google Chrome versions later than version 42. You can use the Internet Explorer version 10 or 11 or Firefox version 46 browser to use the CLI terminal. [PR1283216](#)
- On SRX Series devices, sometimes the time range slider does not work for all events and individual events in Google Chrome and Firefox browsers. [PR1283536](#)

## Network Management and Monitoring

- The `snmpd` process leaks memory in the SNMPv3 query path and crashes. The issue is caused by a memory leak when the request PDU is dropped by SNMP when the **snmp filter-duplicates** configuration is enabled. Each request PDU has a structure pointer for the SNMPv3 security details. This is allocated when the PDU is created or cloned. But while dropping the duplicate requests, the corresponding structure is not freed, which causes the memory leak. [PR1392616](#)

## Platform and Infrastructure

- On SRX Series devices running FreeBSD 6.0 based Junos OS, when a USB flash drive with a mounted file system is physically detached by a user, the system might panic. The issue is resolved with FreeBSD 10 and later (upgraded FreeBSD). [PR695780](#)
- On SRX5800 devices, if the system service REST API is added to the configuration, even though the commit can be completed, all the configuration changes in this commit do not take effect. This occurs because the REST API daemon 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 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 on time, 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 if the % symbol is present in the 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** command might show the same serial number for the second Routing Engines on both the nodes. [PR1321502](#)
- On the SRX4000 line of devices with chassis cluster setup, when more than two ports are bound as reth interfaces on each node, packet drop might be seen. [PR1345941](#)
- When using third-party certificate chain for the Web authentication redirect page, for the HTTP REST API, or for J-Web access, which contains at least one intermediate CA certificate, the SRX Series device does not send the intermediate certificate to the client. [PR1408921](#)
- An MTU change after a CFM session is brought up can impact Layer 2 Ethernet ping (loopback messages). If the new MTU is lower than the original value, then Layer 2 Ethernet ping fails. [PR1427589](#)
- The PICs might go offline and split-brain might be seen when an interrupt storm happens on the internal Ethernet interface `em0` or `em1`. [PR1429181](#)
- Unable to launch J-Web when the device is upgraded using a USB image. [PR1430941](#)

## Routing Policy and Firewall Filters

- An SRX345 device running Junos OS Release 15.1X49-D180 has high NSD usage due to a possible memory leak. [PR1452721](#)
- In a rare case, a specific domain is not resolved by the SRX Series device when using the DNS address book. This is because the DNS library resolver fails to identify the pointer with a big offset in the compressed DNS name. [PR1471408](#)

## VPNs

- On SRX Series devices, if an IPsec VPN tunnel is established using IKEv2, due to a bad SPI, packets might be dropped during CHILD\_SA rekey when the device is the responder for this rekey. As a workaround, to ensure that the SRX Series devices are always the initiator for the CHILD\_SA rekey, by setting the **lifetime-seconds** statement to a lower value than it is set on the remote peer. The **lifetime-seconds** value can be set under **[edit security ipsec proposal]**. [PR1129903](#)
- On SRX Series devices, if multiple traffic selectors are configured for a peer with IKEv2 reauthentication, only one traffic selector rekeys 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 be triggered through other mechanisms such as traffic or peer. [PR1287168](#)
- When using the operational mode **request security ike debug-enable** command for IKE debugging after using IKE traceoptions with a filename specified in the configuration, the debugged files are written to the same filename. [PR1381328](#)
- VPN tunnels flap after a group is added or deleted in edit private mode in a clustered setup. [PR1390831](#)

### RELATED DOCUMENTATION

[New and Changed Features | 4](#)

[Changes in Behavior and Syntax | 4](#)

[Known Limitations | 5](#)

[Resolved Issues | 16](#)

[Documentation Updates | 17](#)

# Resolved Issues

## IN THIS SECTION

- [Application Layer Gateways \(ALGs\) | 16](#)
- [Flow-Based and Packet-Based Processing | 16](#)
- [Routing Policy and Firewall Filters | 17](#)
- [Unified Threat Management \(UTM\) | 17](#)

This section lists the issues fixed in hardware and software in Junos OS Release 15.1X49-D220. For information about resolved issues in Junos OS Release 15.1X49-D10 through Junos OS Release 15.1X49-D210, refer to the [Release Notes](#) listed in the Release 15.1X49 section.

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)

- FTPS traffic might get dropped on SRX Series or MX Series platforms if FTP ALG is used. [PR1483834](#)

## Flow-Based and Packet-Based Processing

- Throughput or latency performance of all traffic drops when TCP traffic is passing through the device. [PR1403727](#)
- The AAMW policy rules for IMAP traffic sometimes might not get applied when traffic passes through SRX Series devices. [PR1450904](#)
- Recent changes to JDPI's classification mechanism caused a considerable performance regression (more than 30 percent). [PR1479684](#)



## Routing Policy and Firewall Filters

- The NSD process might get stuck and cause problems. [PR1458639](#)

## Unified Threat Management (UTM)

- UTM websense redirect supports IPv6 messages. [PR1481290](#)

### RELATED DOCUMENTATION

<a href="#">New and Changed Features   4</a>
<a href="#">Changes in Behavior and Syntax   4</a>
<a href="#">Known Limitations   5</a>
<a href="#">Open Issues   11</a>
<a href="#">Documentation Updates   17</a>

# Documentation Updates

## Chassis Clustering

- On SRX5400, SRX5600, and SRX5800 devices in a chassis cluster, when the PICs containing fabric links on the SRX5K-MPC3-40G10G (IOC3) are powered off to turn on alternate PICs, always ensure that:

The chassis cluster is in dual-homing mode to ensure minimal RTO loss, after alternate links are brought online.

### RELATED DOCUMENTATION

<a href="#">New and Changed Features   4</a>
<a href="#">Changes in Behavior and Syntax   4</a>
<a href="#">Known Limitations   5</a>

# Migration, Upgrade, and Downgrade Instructions

## IN THIS SECTION

- Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 18

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

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 User Guide for Security Devices](#).

RELATED DOCUMENTATION

<i>New and Changed Features</i>
<i>Known Behavior</i>
<i>Known Issues</i>
<i>Resolved Issues</i>
<i>Changes in Behavior and Syntax</i>

# Product Compatibility

IN THIS SECTION

- [Hardware Compatibility | 19](#)
- [Transceiver Compatibility for SRX Series Devices | 20](#)

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

## 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

- **Feature Explorer**—Determine the features supported on MX Series, PTX Series, QFX Series devices. The Juniper Networks Feature Explorer is a Web-based app that helps you to explore and compare Junos OS feature information to find the right software release and hardware platform for your network. <https://pathfinder.juniper.net/feature-explorer/>
- **PR Search Tool**—Keep track of the latest and additional information about Junos OS open defects and issues resolved. [prsearch.juniper.net](https://prsearch.juniper.net).
- **Hardware Compatibility Tool**—Determine optical interfaces and transceivers supported across all platforms. [apps.juniper.net/hct/home](https://apps.juniper.net/hct/home)

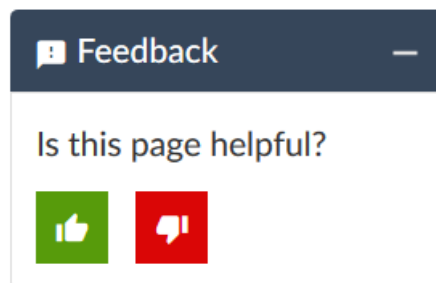
**NOTE:** To obtain information about the components that are supported on the devices, and the special compatibility guidelines with the release, see the Hardware Guide for the product.

- **Juniper Networks Compliance Advisor**—Review regulatory compliance information about [Common Criteria](#), [FIPS](#), [Homologation](#), [RoHS2](#), and [USGv6](#) for Juniper Networks products. [apps.juniper.net/compliance/](https://apps.juniper.net/compliance/).

## 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 system—Click TechLibrary Feedback, on the lower right of any page on the [Juniper Networks TechLibrary](#) site, and do one of the following:



- Click the thumbs-up icon if the information on the page was helpful to you.
- Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.
- E-mail—Send your comments to [techpubs-comments@juniper.net](mailto: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 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://support.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](mailto:support@juniper.net). For documentation issues, fill out the bug report form located at <https://www.juniper.net/documentation/feedback/>.

# Revision History

7, July 2020—Revision 2— Junos OS 15.1X49-D220 – SRX Series.

1, June 2020—Revision 1— Junos OS 15.1X49-D220 – SRX Series.

Copyright © 2020 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.