Release Notes: Junos® OS Release 15.1X49-D150 for the SRX Series

Release 15.1X49-D150
31 January 2019
Revision 5

Contents

Introduction

Junos OS runs on the following Juniper Networks® 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-D150 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-D150 supports the following devices: SRX300, SRX320, SRX340, SRX345, and SRX550 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 SRX 5400, 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-D150 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-D140, refer to the Release Notes listed in the Release 15.1X49 section at Junos OS for SRX Series page.

- Release 15.1X49-D150 Software Features on page 4

Release 15.1X49-D150 Software Features

AppSecure

Application Quality of Experience (SRX300, SRX320, SRX340, SRX345, SRX550M, SRX1500, SRX4100 SRX4200, and vSRX)—Starting in Junos OS Release 15.1X49-D150, AppQoE enables you to effectively prioritize, segregate, and route business-critical applications traffic without compromising performance or availability.

AppQoE utilizes the capability of application identification and advanced policy-based routing to identify specific applications in the network and to specify a path for the application traffic according (service-level agreement) SLA rules.

AppQoE monitors RTT, jitter, and packet loss on each link, and based on the score, seamlessly diverts applications to an alternate path if the performance of the primary link is below acceptable levels as specified by the SLA. Measurement and monitoring of application performance is done using active and passive probes, which detect SLA violations and help select an alternate path for that particular application.

[See Application Quality of Experience.]

Related Documentation

- Migration, Upgrade, and Downgrade Instructions on page 16
- Changes in Behavior and Syntax on page 4
- Known Behavior on page 5
- Known Issues on page 9
- Resolved Issues on page 13

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-D150.

AppSecure

- **Passive packet probe**—Starting from Junos OS Release 15.1X49-D150, on all supported SRX Series devices and vSRX instances, in order to detect if a link or path is down by passive probes, a minimum of three probe requests and 100% packet loss must occur in a sampling period for a given session to trigger SLA violation.

  [See Application Quality of Experience.]

Installation and Upgrade

- Post configuration scripts from ZTP are not able to run on SRX300 devices.

  [See Zero Touch Provisioning on SRX Series Devices.]

SNMP

- **SNMP traps sent from backup node, too (SRX Series)**—Starting in Junos OS Release 15.1X49-D150, for SRX clusters, the backup node runs as a separate entity; therefore, traps need to be sent from the cluster's backup node as well as from the primary node. Previous to this fix there was a block on backup nodes sending SNMP traps to the network management system. The current fix removes this block.

  [See Example: Configuring Chassis Cluster Redundancy Group IP Address Monitoring.]

System Logs

- **System log host support (SRX300, SRX320, SRX340, SRX345 Series devices)**— Starting in Junos OS Release 15.1X49-D150, when the device is configured in stream mode, you can configure maximum of eight system log hosts.

  In Junos OS Release 15.1X49-D140 and earlier releases, you can configure only three system log hosts in the stream mode. If you configure more than three system log hosts, then the following error message is displayed **error: configuration check-out failed**.

Related Documentation

- New and Changed Features on page 4
- Known Behavior on page 5
- Known Issues on page 9
- Resolved Issues on page 13
- Migration, Upgrade, and Downgrade Instructions on page 16

Known Behavior

This section contains the known behaviors, system maximums, and limitations in hardware and software in Junos OS Release 15.1X49-D150.

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

- On SRX550M devices in 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 interfaces configured on each node, which enables an RLAG (Redundant Link Aggregation). 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 device will drop the response packets. PR1344173

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

Flow-Based and Packet-Based Processing

- On SRX5400, SRX5600, and SRX5800 devices, in a central point architecture, system logs are sent per second per SPU. Hence, the number of SPUs defines the number of system logs per second. PR1126885
- On all SRX Series devices, when using event mode logging, some AppTrack log messages might be lost in case of heavy logging. As a result, the Packet Forwarding Engine might send the messages in batches, overflowing the log buffer on the Routing Engine. The log buffer size is increased as a mitigation, but in rare situations some log messages might still be dropped. PR1133757
- On SRX5400 devices, if a user or a group name contains the following characters: **"*" (ASCII 0x2a), "(" (ASCII 0x28), ")" (ASCII 0x29), "\" (ASCII 0x5c) and NUL (ASCII 0x00)**, the query from the device to the LDAP server might time out, leading to a high CPU utilization. PR1157073
- · 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 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 SRX Series devices, OSPF over GRE over IPsec is not supported on a device with a standalone central point. PR1274667

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 ageout 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, 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 st0 interface and the incoming traffic rate destined for 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. It is recommended you configure appropriate policer on the ingress interface to limit the traffic below 300,000 pps per SPU. PR1239021

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, DHCP client bindings under Monitor is removed. The same bindings can be seen in the output of the **show dhcp client binding** CLI command. PR1205915
- On SRX Series devices, adding 2000 global addresses at a time to the SSL proxy profile exempted addresses can cause the Web page 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

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 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 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 Series 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 SRX1500 devices, when the CPU usage is very high (above 95 percent), there is a possibility that the connection between AAMW and PKID process can stop. In this case, the AAMW process remains in an initializing state until the connection is established. PR1142380

VPNs

- On SRX Series devices, if an IPsec VPN tunnel is established using IKEv2 because of bad SPI, packet drop might be observed during the **CHILD_SA rekey** when the device is the responder for this rekey. PR1129903
- On SRX1500 devices in a chassis cluster with Sky ATP solution deployed, if you disable and then reenable the CRL checking of certificate validity, the system does not reenable the CRL checking. PR1144280

Related Documentation

- New and Changed Features on page 4
- Changes in Behavior and Syntax on page 4
- Known Issues on page 9
- Resolved Issues on page 13
- Migration, Upgrade, and Downgrade Instructions on page 16

Known Issues

This section lists the known issues in hardware and software in Junos OS Release 15.1X49-D150.

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 in chassis cluster mode, the IOC cards might stop during an RG0 failover. PR1359641

Flow-Based and Packet-Based Processing

- On SRX Series devices, sometimes the time range slider does not work for all events and for individual events in the Google Chrome or the Firefox browser. PR1283536
- On SRX Series devices with chassis cluster enabled in active-active mode, when multicast traffic crosses multiple logical-systems (LSYS) and also crosses the fabric link (Z-mode traffic), some sessions may not be cleared after ageout. PR1295893
- On SRX Series devices, when chassis cluster is enabled, there is a small time window during the RG0 failover when the value of the non-maskable interrupt (NMI) is incorrect, resulting in the IOC cards to stop. PR1359641
- In an active-active chassis cluster mode when an IPsec tunnel is configured, the cleartext packets entering into the backup redundancy group are forwarded to the active redundancy group node for packet encryption through the chassis cluster fabric link. Thus, the packets are sent out through the wrong chassis cluster node and disturb the IPsec sequence number for the tunnel session. At last, packet loss is observed from receiver side. PR1373161
- When using the user firewall device identity feature, a valid username learned by the PC probe is replaced by the null username. PR1375514

Interfaces and Chassis

- On SRX300, SRX320, SRX340, SRX345, and SRX550M devices, for logical interface scaling, without the **per-unit-scheduler** configured, the total logical interface number is limited to 2048 and with the **per-unit-scheduler** configured on the physical interface, the total logical interface number is limited to CoS scheduler sub-unit upper limit (2048). So, the logical interface **max-number** for the **per-unit scheduler** should be 2048 minus the number of physical interface (which is up with at least one logical interface up, max number is 128). PR1138997
  - Without **per-unit-scheduler** configured, total IFL number is limited to 2048.
  - With **per-unit-scheduler** configured on the IFD interface: total IFL number is limited to CoS scheduler **sub-unit** upper limit (2048). So, IFL **max-number** for **per-unit-scheduler** should be 2048 minus the number of physical interface (which is up with at least one logical interface up, maximum number is 128).
- The following message appears for each port whose settings are changed or refreshed:

  Apr 3 12:00:00 srx /kernel: check_configured_tpids: <interface> : default tpid (0x8100) not configured. pic allows maximum of 0 tpids
  Apr 3 12:00:00 srx /kernel: check_configured_tpids: <interface> number of configured tpids exceeds the limit(0)

  PR1373668

J-Web

- 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, an issue occurs when you log in to J-Web and navigate to Monitor > Services > DHCP > DHCP SERVER & DHCP RELAY. When you click the Help page icon, the Online Help page displays a 404 error message. PR1267751
- 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
- The J-Web setup wizard does not propagate the DHCP attributes from ISP to LAN. PR1370700

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, 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
- On SRX5400, SRX5600, and SRX5800 devices in chassis cluster mode, when the em interface is down, the control links are lost and the device cluster is in an abnormal state. PR1342362
- 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 as the program PHP cannot exit properly. Therefore, the system creates a new httpd process to handle the new Web authentication requests. PR1352894

System Logs

- The following warning syslog message is displayed when the number of security screens installed exceeds the IOC capacity. **node0.fpc5 System supports up to 1024 policer groups, currently 2000 policer groups are allocated.Please reduce the number of flooding type screens.** PR1209565

Unified Threat Management (UTM)

- On SRX Series devices, if advanced antimalware service is enabled, and the SMTP is configured in the antimalware service policy with fallback permission enabled under the long network latency between the devices and AWS running Juniper Sky ATP service, there might be a file submission timeout error. When sending the timeout error message, there is a possibility that the e-mail sent from Outlook might remain in the outbox of the sender, and the receiver might not receive the e-mail. PR1254088

Upgrade and Downgrade

- On SRX550M devices, when you upgrade from Junos OS Release 15.1X49-D30 to a later Junos OS release, the upgrade fails. PR1237971

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 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
- If the certificate authority (CA) profile name has a period (.), then the PKI process encounters issues if it is restarted. PR1351727

Related Documentation

- New and Changed Features on page 4
- Changes in Behavior and Syntax on page 4
- Known Behavior on page 5
- Resolved Issues on page 13
- Migration, Upgrade, and Downgrade Instructions on page 16

Resolved Issues

This section lists the issues fixed in hardware and software in Junos OS Release 15.1X49-D150. For information about resolved issues in Junos OS Release 15.1X49-D10 through Junos OS Release 15.1X49-D140, 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)

- On SRX5400, SRX5600, and SRX5800 devices with ike-esp-nat ALG enabled, the IPsec packet might be dropped after an IKE or IPsec security association (SA) renegotiation because of a session conflict. PR1372232

Application Security

- If the serial number of the certificate for SSL proxy has two consecutive zeros, then the certificate authentication fails. PR1328253

Chassis Cluster

- IPv6 backup sessions might be stuck and cannot be cleared after the data plane redundant group failover. PR1354448
- On SRX Series devices in chassis cluster mode, if IP monitoring is enabled, the cluster becomes unresponsive after an upgrade due to a memory leak issue. PR1366958
- On SRX Series devices in chassis cluster mode, with a large number of BGP peers and IPsec tunnels, some traffic crossing the fabric link (Z-mode traffic) might be lost after a failover of redundancy group 0. PR1377266

Dynamic Host Configuration Protocol

- SRX300, SRX320, SRX340, and SRX345 devices with LTE mPIM do not forward the DHCP relay packets over the LTE. PR1357137

Flow-based and Packet-based Processing

- 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
- Cflow cannot configure the source address for flow packets. PR1328565
- On SRX300, SRX320, SRX340, SRX345, and SRX550M devices, the RPD process might stop when configuring the auto-bandwidth option under the label-switched path in MPLS. PR1331164

- SSH to the loopback interface of the device does not work properly when the application tracking is configured PR1343736
- SNMP MIB walk provides wrong data counter for the total number of current flow sessions. PR1344352
- On SRX300, SRX320, SRX340, and SRX345 devices, unable to lock-down the USB port. PR1352104
- The flowd process might stop when an ALG is enabled. PR1352416
- When the routing instance is configured, the UTM antispam does not send the DNS query. PR1352906
- On SRX Series devices, the flowd process might stop. PR1353184
- The IPv6 backup sessions might be stuck and cannot be cleared after the data-plane redundancy group failover. PR1354448
- Traffic does not match if the following error message appears: **Policy is out of sync between RE (Routing Engine) and PFE (Packet Forwarding Engine) node0.fpc0. Please resync before commit**. PR1355528
- The PIM register message from source first-hop router (FHR) suddenly stops appearing. PR1356241
- On SRX Series devices, in an SSL proxy scenario, if the TLS packets contain application layer protocol negotiation (ALPN), then the ALPN extension is removed by the SSL proxy, resulting in the negotiation failure of the application layer protocol. PR1360820
- SNMP MIB walk does not work when screens are applied to more than 14 security zones. PR1364210
- A flowd core file is generated after an RG0 failover. PR1366122
- If the **phone-home: kern.maxfiles** limit is exceeded then SSH failure occurs. PR1357076

Forwarding and Sampling

- The microkernel leaks 6x40 bytes of heap nodes upon each IPC path during handshake or establishment between L2ALM and L2ALD. PR1326921

Interfaces and Routing

- The **set protocols rstp interface all** command works incorrectly. PR1355586
- The SRX Series device might wrongly flood the broadcast frames if the frames are received on the VPLS interface. PR1350857
- On SRX1500 devices, the ae0 and ae1 interfaces display the MAC address as 00:00:00:00:00:00 and 00:00:00:00:00:01. PR1352908
- On SRX1500 devices, the port LED does not turn on although the interface is logically up. PR1364754

Intrusion Detection and Prevention (IDP)

- IDP signature update fails on the secondary node. PR1358489

J-Web

- On all SRX Series devices, after you run the **request system zeroize** command, the J-Web interface is not accessible. PR1335561
- When the J-Web fails to get the resource information, the Routing Engine CPU usage shows 100% in resource utilization in the J-Web dashboard. PR1351416
- The J-Web menu at the security policies search button does not work when using the Internet Explorer version 11. PR1352910

Layer 2 Ethernet Services

- The subnet mask is not sent as the reply to a **DHCPINFORM** message. PR1357291

Platform and Infrastructure

- When you commit an **apply-groups** configuration, the VPN connection flaps. PR1242757
- The device clock might not synchronize with the NTP server. PR1357843
- Frequency logs are displayed on the SRX5400, SRX5600, and SRX5800 devices when the IOC card has the same identifier as the SPC PIC card. PR1357913
- The output of the **show interfaces extensive** command displays ge interfaces operating in half duplex mode, even when the link is operating as full duplex. This is a display issue and does not impact traffic. PR1358066
- The SCP configuration backup fails even though the **/var/etc/ssh_known_hosts** has a proper fingerprint. PR1359424

Routing Policy and Firewall Filters

- The VNC application matching now includes both TCP/5800 and TCP/5900 ports. PR1333206
- On SRX Series devices, the nsd process might crash on the Packet Forwarding Engine with large-scale security policy configuration. PR1354576
- The timeout value of **junos-http** is incorrect. PR1371041

Routing Protocols

- The ppmd process might stop during ISSU. PR1347277
- On SRX1500 devices, dedicated BFD does not work. PR1347662

Unified Threat Management (UTM)

- The default action of Web filtering does not work as expected. PR1365389

VLAN Infrastructure

- The flowd process might stop when destination MAC addresses are matched in a device operating in transparent mode. PR1355381

VPNs

- Commit does not consider IKE logical gateway interface (redundant Ethernet interface) configuration dependency upon deletion of the reth interface from the configuration. PR1352559
- The IPsec VPN traffic might be dropped on the pass-through device after an IKE rekey operation. PR1353779
- 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
- Changes in Behavior and Syntax on page 4
- Known Behavior on page 5
- Known Issues on page 9
- Migration, Upgrade, and Downgrade Instructions on page 16

Documentation Updates

There are no errata or changes in Junos OS Release 15.1X49-D150 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 17

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 4
- Known Behavior on page 5
- Known Issues on page 9
- Resolved Issues on page 13

Product Compatibility

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

- Hardware Compatibility on page 18
- Transceiver Compatibility for SRX Series Devices on page 18

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, 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 5— Junos OS 15.1X49-D150 – SRX Series.

30, January 2019—Revision 4— Junos OS 15.1X49-D150 – SRX Series.

28, January 2019—Revision 3— Junos OS 15.1X49-D150 – SRX Series.

24, December 2018—Revision 2— Junos OS 15.1X49-D150 – SRX Series.

19, September 2018—Revision 1— Junos OS 15.1X49-D150 – SRX Series.