Release Notes: Junos® OS Release 15.1X49-D180 for the SRX Series

Release 15.1X49-D180
06 April 2020
Revision 3

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-D180 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-D180 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/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

This section describes the new features and enhancements to existing features in Junos OS Release 15.1X49-D180 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-D160, refer to the Release Notes listed in the Release 15.1X49 section at Junos OS for SRX Series page.

Release 15.1X49-D180 Software Features

There are no new features in Junos OS Release 15.1X49-D180 for the SRX Series devices.

RELATED DOCUMENTATION

Migration, Upgrade, and Downgrade Instructions | 19

Changes in Behavior and Syntax | 4

Documentation Updates | 19

Known Behavior | 6

Resolved Issues | 16

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-D180.

Authentication and Access Control

- **Enhanced output for show security firewall-authentication jims statistics (SRX Series)**—Starting in Junos OS Release 15.1X49-D180, the output for the **show security firewall-authentication jims statistics** operational command is enhanced to display the statistics of both the primary and secondary JIMS servers. For example, the **show security firewall-authentication jims statistics** operational command displays the following sample output:

```
root@user> show security firewall-authentication jims statistics
```

```
Primary server:
  Push success counter: 1
  Push failure counter: 0

Secondary server:
  Push success counter: 1
  Push failure counter: 0
```

[See show security firewall-authentication jims statistics.]

Network Management and Monitoring

- **NSD Restart Failure Alarm (SRX Series)**—Starting in Junos OS Release 15.1X49-D180, a system alarm is triggered when the Network Security Process (NSD) is unable to restart due to the failure of one or more NSD subcomponents. The alarm logs about the NSD are saved in the messages log. The alarm is automatically cleared when NSD restarts successfully.

  The **show chassis alarms** and **show system alarms** commands are updated to display the following output when NSD is unable to restart - **NSD fails to restart because subcomponents fail**.

  [See Alarm Overview.]

RELATED DOCUMENTATION

New and Changed Features | 4

Migration, Upgrade, and Downgrade Instructions | 19

Documentation Updates | 19

Known Behavior | 6

Known Behavior

This section contains the known behaviors, system maximums, and limitations in hardware and software in Junos OS Release 15.1X49-D180.

Authentication and Access Control

- On SRX Series devices, TLS1.0 and TLS1.1 SSL protocols are blocked because of reported security vulnerabilities. This change might affect users accessing J-Web, Web authentication GUI, or using Dynamic VPN through Pulse client, when using an older OS or lower version browsers where TLSv1.2 protocol is not supported. This change affects Junos OS Release 12.3X48-D55, 15.1X49-D100, and all higher SRX Series releases. PR1283812

Chassis Clustering

- On SRX550M devices in a chassis cluster, traffic loss for about 10 seconds is seen when there is power failure on the active chassis cluster node. PR1195025
- On all SRX Series branch devices, if you enable **ip monitoring** for redundancy groups, the feature might not work properly on the secondary node if the reth interface has more than one physical interface configured. This is because the backup node will send 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 will drop it. PR1344173
- For HA cold synchronization, the GTP-U session will be synchronized to the secondary device before the GTP-U tunnel, which will cause GTP-U tunnel cannot be linked with the corresponding GTP-U flow session, then GTP-U tunnel will not get refreshed by GTP-U traffic until new sessions are created. If old sessions do not get age out on the primary device, all GTP-U traffic will go through fast path and no session creation events are triggerd then after the GTP-U timeout period, the tunnels on the secondary device will be aged out earlier. PR1353791

Flow-Based and Packet-Based Processing

- 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 will 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 SRX1500 devices, when a 1-Gigabit Ethernet SFP-T is used on 1-Gigabit Ethernet SFP ports (ge-0/0/12 to ge-0/0/15), the ge interface does not operate at 100-Mbps speed. PR1133384
- On all SRX Series devices, when using event mode logging, some AppTrack log messages may be lost in case of heavy logging. The reason is that the Packet Forwarding Engine may 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 occasions the dropping of some log messages may still occur. PR1133757
- On SRX1500 devices, when CPU usage is very high (above 95 percent), there is a possibility that the connection between the AAMW process and PKI daemon can 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. It is recommended to change 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 Juniper Sky Advanced Threat Prevention (ATP) solution deployed, if you disable and then reenable CRL checking of certificate validity, the system does not reenable 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 following characters * **(ASCII 0x2a)**, **(ASCII 0x28)**, **(ASCII 0x29)**, \ **(ASCII 0x5c)** and NUL (ASCII 0x00), the query from the device to the LDAP server will time out and might lead to high CPU utilization. PR1157073
- On SRX Series devices, after the 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 changing 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 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, 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 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 17,000 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, and SRX1500 devices, in vSRX 2.0 the command **set system internet-options tcp-mss < value >** does not work in Junos OS Release 15.1X49. PR1213775
- On SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices, VPLS traffic forwarding stops working after enabling Ethernet-switching configuration. VPLS and Ethernet-switching must not be configured together on the same device. It is recommended to avoid using a Ethernet-switching configuration on these platforms when VPLS is enabled. PR1214803
- 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
- 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
- On SRX Series devices, if advanced anti-malware service (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 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
- A modem profile is not active until a profile is defined. You need to define a profile before selecting a profile. PR1254427
- 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
- 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 recommended using only one LTE mPIM in the supported devices. PR1262543
- On SRX Series devices, OSPF over GRE over IPsec is not supported on a device with a standalone central point. PR1274667
- A FIPS core file is seen 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, AAMW established sessions always use the configured AAMW parameters at the time of session establishment. 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

- On SRX Series devices, you cannot view the custom log files created for event logging in J-Web. PR1280857
- On SRX Series devices, firewall-authentication cannot retrieve domain information from the access profile configuration, 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 a LDAP access profile. PR1281063
- The user-firewall process useridd will keep retrying connecting to AD server when it fails to connect to the server. This makes useridd is unable to handle other messages. Therefore the administrator must remove or deactivate those unused/incorrect user-firewall configuration. 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
- On SRX Series devices running with Junos OS Release 15.1X49-D90 and earlier releases, J-Web often does not display IDP log locally saved. PR1336341
- On SRX Series devices, if a Point-to-Point Protocol interface is used, some packets of a stream received on the PPP interface will get re-ordered, which can cause issues to certain applications (for example, TV conference systems). PR1340417
- FTP using Micorosoft NLB does not work correctly in transparent mode. PR1341446
- The SRX Series devices does not get the built-in domain computers group for the new computers added to the domain. PR1361512
- The interface cannot up when you change from 10m to 100m when using the crossover cable. PR1387978
- When using Advanced, application based, Multipath routing, the sender sequences packets in order and delivers it to the receiver. If the receiver receives the packets out of order, then in the current release it is designed to drop the packets. Since IPSEC may reorder the packets coming out of the sender for fragmented packets, it may get dropped at the receiver. PR1403584
- Packet might be dropped in SD-WAN use case if there is no IPsec configured ((for example, IP over MPLS over GRE) in HA Z mode. Issue will not be seen if IPsec is configured (IP over MPLS over GRE over IPSec) or in chassis cluster active/passive mode. PR1415343

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, the 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 CLI using the **show dhcp client binding** command. PR1205915
- On SRX Series devices, when you log in to J-Web and navigate to **Monitor->Services->DHCP->DHCP Relay**, when you 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

Platform and Infrastructure

- On SRX5800 devices, if a global SOF policy (all session service-offload) is enabled, the connections per second 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 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

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 may occur when a protocol does not predeclare the content size. PR1005086

VPNs

- On SRX Series devices, if an IPsec VPN tunnel is established using IKEv2, due to bad SPI, packet drop might be observed during CHILD_SA rekey when the device is the responder for this rekey. PR1129903
- On SRX Series devices, an IPsec VPN tunnel which uses a PPPoE interface as the external interface will fail after RG0 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 3,00,000 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 an appropriate policer on the ingress interface to limit the traffic below 3,00,000 pps per SPU. PR1239021

RELATED DOCUMENTATION

New and Changed Features | 4

Migration, Upgrade, and Downgrade Instructions | 19

Changes in Behavior and Syntax | 4

Known Behavior | 6

Resolved Issues | 16

Known Issues

This section lists the known issues in hardware and software in Junos OS Release 15.1X49-D180.

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)

- When both ALG and **rst-invalidate-session** are enabled, the TCP reset packet will be dropped by the SRX Series devices. This will impact all TCP ALG related traffic. PR1430685

Flow-Based and Packet-Based Processing

- 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 the commit will not take effect. This occurs because the REST API process 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 SRX300, SRX320, SRX340, SRX345, and SRX550M devices, for IFLS (logical interface) scaling without **per-unit-scheduler** configured, the total IFL number is limited to 2048. With **per-unit-scheduler** configured on the IFD interface. The total IFL number is limited to the CoS scheduler sub-unit upper limit is 2048. So, the 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, the maximum number is 128. PR1138997
- On SRX1500 devices in a chassis cluster with Juniper Sky Advanced Threat Prevention (ATP) solution deployed, if you disable and then reenable CRL checking of certificate validity, the system does not reenable CRL checking. PR1144280
- 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 advanced anti-malware service (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 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, sometimes the time range slider does not work for all events and individual events in Google Chrome or Firefox browsers. 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
- IDP install fails on one node due to AppID process gets stuck. PR1336145
- The issue affects all SRX platforms if doing an ISSU upgrade. The reth interface might flap and cause traffic loss. PR1381475
- On SRX300 line devices, the default configuration changed. PR1393683

- Multipath credit limit might get reset after multiple configuration changes and interface flaps. While there is no proper sequence of steps that cause it, the credit limit might get reset considering the default interface speed of 1 Gbps and default/configured bandwidth limit. PR1401090
- When utilizing services that are reliant on TCP proxy, such as SSL-FP, SAV, or Juniper Sky ATP in block-mode, during times of congestion, downloads may stall or completely fail. PR1403412
- On SRX1500 platforms, when you configure **interface-mac-limit** on one interface and then send traffic with different source MAC (such as 10,000) to the interface. The number of learned MAC addresses reach max-value limit (8192). Traffic cannot transfer on all interfaces. PR1409018
- On SRX Series devices, the result of MIB OID **dot3StatsDuplexStatus** shows full duplex for the interface which the status is half duplex due to auto negotiation failure. PR1409979
- On all SRX Series platforms, in 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 may get dropped due to reroute failure. PR1410233
- Stream mode syslog messaging is not escaping the \ correctly PR1416093
- GRE packets are being dropped before entering the IPsec tunnel after reboot or restart of routing process. PR1423768
- There are same type of Kernel messages seen in the syslogs alerting of PKI daemon usage. PR1426791

Interfaces and Chassis

- The **monitor interface** command will start the ifmon process. In this time if telnet session to the router is disconnected unconventionally, then the ifmon process was not killed and it will take 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

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 Configure> Security> Security Policy page. PR1251714
- On SRX Series devices, 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 initially show no data available even when the device has a large amount of data. Refreshing the individual widgets to show the data. PR1282666
- On SRX Series devices, the CLI terminal does not work for Google Chrome version later than 42. You can use Internet Explorer 10 or 11 or Firefox 46 browsers to use the CLI terminal. PR1283216
- On SRX Series devices, J-Web incorrectly displays port-mode **access** for the link aggregation interfaces despite them being configured with multiple vlan-ids and port-mode **trunk**. This is a display issue and does not impact the operation of the interface. PR1430414

Platform and Infrastructure

- On SRX Series devices running FreeBSD 6-based Junos OS software, when a USB flash device with a mounted file system is physically detached by a user, the system might panic. The issue is resolved with FreeBSD 10 and later. Please contact JTAC for confirmation if the code and platform in your case is running FreeBSD 10 or later. PR695780
- 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 CLI with **%** 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** operational command may show the same serial number for both the second Routing Engines on both the nodes. PR1321502
- On SRX4100 and SRX4200 devices, when the power is removed from a power supply, no SNMP trap would be sent out to report the failure. This issue only affects Junos OS Release 15.1X49 release train, no later releases would be affected. PR1362973
- Login class with allowed-days and specific access-start/access-end does not work as expected. PR1389633

Routing Policy and Firewall Filters

- When the alarm message **NSD fails to restart because subcomponents fail** happens, a new alarm **NSD fails to restart because subcomponents fail** is triggered. This alarm will be cleared automatically when NSD can restart successfully. PR1422738

Unified Threat Management (UTM)

- From Junos OS Release 18.4 and above release, UTM log includes source and destination zone information. PR1326271
- On Junos OS Release 18.2R3 release on SRX300 platform, when system only install UTM license, it needs system to be rebooted twice to make system run in advance mode, if system installed IDP license (with or without install UTM license), it only need one time reboot to get system work in advance service mode. Advanced service mode means, more memory/packet buffer for advanced service like IDP/UTM (with session capacity cut to half). PR1429296

VPNs

- On SRX Series devices, if an IPsec VPN tunnel is established using IKEv2, due to bad SPI, packet drop might be observed during CHILD_SA rekey when the device is the responder for this rekey. PR1129903
- On SRX Series devices, in case 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 will be cleared without immediate rekey. New negotiation of those traffic-selectors might trigger through other mechanisms such as traffic or by peer. PR1287168
- Use the file created under **set security ike traceoptions** file to check the logs. PR1381328
- VPN tunnels flap after adding or deleting a group in **edit private** mode on a clustered setup. PR1390831
- VPN does not recover on the high-end standalone SRX Series devices when the CLI operation **restart ipsec-key-management** is done. PR1400712

RELATED DOCUMENTATION

New and Changed Features | 4

Migration, Upgrade, and Downgrade Instructions | 19

Resolved Issues

This section lists the issues fixed in hardware and software in Junos OS Release 15.1X49-D180. For information about resolved issues in Junos OS Release 15.1X49-D10 through Junos OS Release 15.1X49-D170, 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 Firewall

- Fail to match permit rule in AppFW rule set. PR1404161

Application Layer Gateways (ALGs)

- On all SRX Series platforms, SIP/FTP ALG does not work when SIP traffic with source NAT goes through the SRX Series devices. PR1398377
- DNS requests with the EDNS option might be dropped by the DNS ALG. PR1379433

Chassis Clustering

- The flowd process stops when updating or deleting a GTP tunnel. PR1404317
- The SRX Series devices might be potentially overwritten with an incorrect buffer address when detailed logging is configured under the GTPv2 profile. PR1413718
- Traffic would be dropped if SOF is enabled in a chassis cluster in active/active mode. PR1415761
- From Junos OS Release 18.4, at most 6 pdn connects can be contained in a pdp context response. Otherwise, the response will be dropped. PR1422877

Flow-Based and Packet-Based Processing

- On SRX1500 devices, the activity LED (right LED) for 1-Gigabit Ethernet/10G-Gigabit Ethernet port is not on although traffic is passing through that interface. PR1380928
- SRX1500 went into DB mode after USB installation. PR1390577
- SRX Series device cannot obtain IPv6 address through DHCPv6 when using a PPPoE interface with a logical unit number greater than 0. PR1402066
- Memory leak if AAMW is enabled PR1409606
- The command **show security firewall-authentication jims statistics** will output statistics of both the primary JIMS server and secondary JIMS server. PR1415987
- The TCP session might not get cleared even after it reaches the timeout value. PR1416385
- Traffic logging shows service-name **junos-dhcp-server** for UDP destination port 68. PR1417423
- Traffic might be lost on the SRX Series device if IPsec session affinity is configured with **ipsec-performance-acceleration**. PR1418135
- Midplane FRU model number is not displayed. PR1422185
- Partial traffic might get dropped on an existing LAG. PR1423989
- Alarms due to high temperature when operating with expected temperatures. PR1425807

J-Web

- The httpd-gk process crashes, leading to dynamic VPN failures and high Routing Engine CPU utilization upto 100 percent. PR1414642
- J-Web configuration change for an address set using the search function results in a commit error. PR1426321

Network Management and Monitoring

- The **set system no-redirects** setting does not take effect for the reth interface. PR894194

Platform and Infrastructure

- Memory leak might occur on the data plane during composite next hop installation failure. PR1391074
- Complete device outage might be seen when an SPU vmcore is generated. PR1417252
- On SRX Series device, flowd process stops might be seen. PR1417658

Routing Policy and Firewall Filters

- Memory leak in nsd causes configuration change not taking effect after a commit. PR1414319

Routing Protocols

- The rpd process stops after a duplicate secondary route a deleted. PR1113319

Unified Threat Management (UTM)

- The device may not look up the blacklist first in the local Web filtering environment. PR1417330

RELATED DOCUMENTATION

New and Changed Features | 4

Migration, Upgrade, and Downgrade Instructions | 19

Changes in Behavior and Syntax | 4

Known Behavior | 6

Documentation Updates

There are no errata or changes in Junos OS Release 15.1X49-D180 for the SRX Series documentation.

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

Product Compatibility

IN THIS SECTION

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.
- **Hardware Compatibility Tool**—Determine optical interfaces and transceivers supported across all platforms. apps.juniper.net/hct/home

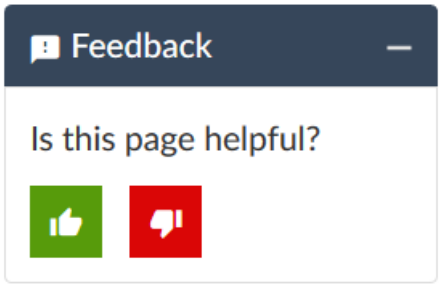
  > **NOTE:** To obtain information about the components that are supported on the devices, and the special compatibility guidelines with the release, see the Hardware Guide for the product.

- **Juniper Networks Compliance Advisor**—Review regulatory compliance information about Common Criteria, FIPS, Homologation, RoHS2, and USGv6 for Juniper Networks products. apps.juniper.net/compliance/.

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. 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. For documentation issues, fill out the bug report form located at https://www.juniper.net/documentation/feedback/.

Revision History

06, April 2020—Revision 3— Junos OS 15.1X49-D180 – SRX Series.

26, November 2019—Revision 2— Junos OS 15.1X49-D180 – SRX Series.

23, May 2019—Revision 1— Junos OS 15.1X49-D180 – SRX Series.