Release Notes: Junos® OS Release 15.1X49-D60 for the SRX Series

Release 15.1X49-D60
13 March 2019
Revision 6

Contents

Introduction 4
New and Changed Features 5
Release 15.1X49-D60 Software Features 6
Application Layer Gateways (ALGs) 6
AppSecure 6
Authentication and Access Control 6
Class of Service 7
Flow-based and Packet-based Processing 7
Interfaces 8
J-Web 9
Multicast 9
NAT 9
Public Key Infrastructure 9
Sky Advanced Threat Prevention 10
VPNs 10
Changes in Behavior and Syntax 11
Application Layer Gateway 11
AppSecure 11
Authentication, Authorization and Accounting (AAA) 12
Chassis Cluster 12
CLI 12
Dynamic Host Configuration Protocol (DHCP) 13
Flow-based and Packet-based Processing 13
Installation and Upgrade 14
Interfaces and Routing 15
Intrusion Detection and Prevention (IDP) 15
Junos OS XML API and Scripting 17
J-Web 17
Layer 2 Features 17
MPLS 18

Multicast . . . 18
NAT . . . 18
Network Time Protocol . . . 20
Public Key Infrastructure . . . 20
Screen . . . 20
System Logs . . . 20
System Management . . . 21
Unified Threat Management (UTM) . . . 21
User Interface and Configuration . . . 23
VPNs . . . 23
Zones and Interfaces . . . 23
Known Behavior . . . 23
AppSecure . . . 23
Attack Detection and Prevention (ADP) . . . 24
CLI . . . 24
Class of Service . . . 24
Flow-based and Packet-based Processing . . . 25
General Packet Radio Service (GPRS) . . . 26
Integrated User Firewall . . . 26
IP Monitoring . . . 26
Layer 2 Features . . . 26
Multicast . . . 27
Platform and Infrastructure . . . 28
Software Installation and Upgrade . . . 28
USB autoinstallation . . . 28
VPN . . . 28
Known Issues . . . 29
Chassis Clustering . . . 29
Command-Line Interface (CLI) . . . 29
Dynamic Host Configuration Protocol (DHCP) . . . 30
Flow-based and Packet-based Processing . . . 30
Interfaces . . . 31
J-Web . . . 31
Layer 2 Ethernet Services . . . 32
Network Address Translation (NAT) . . . 32
Network Management and Monitoring . . . 33
Platform and Infrastructure . . . 33
Routing Policy and Firewall Filters . . . 34
System Logs . . . 34
Unified Threat Management (UTM) . . . 34
VPNs . . . 34
Resolved Issues . . . 35
Resolved Issues . . . 35
Application Layer Gateways (ALGs) . . . 35
Authentication and Access Control . . . 36
Chassis Cluster . . . 36
Flow-based and Packet-based Processing . . . 36
Infrastructure . . . 38
Interfaces . . . 38

Intrusion Detection and Prevention (IDP) . . . 39
J-Web . . . 39
Layer 2 Features . . . 39
Network Address Translation (NAT) . . . 39
Network Management and Monitoring . . . 39
Platform and Infrastructure . . . 40
Routing Policy and Firewall Filters . . . 41
User Interface and Configuration . . . 41
Unified Threat Management (UTM) . . . 41
VPNs . . . 41
Documentation Updates . . . 41
Migration, Upgrade, and Downgrade Instructions . . . 43
Upgrade for Layer 2 Configuration . . . 43
Upgrade and Downgrade Scripts for Address Book Configuration . . . 43
About Upgrade and Downgrade Scripts . . . 44
Running Upgrade and Downgrade Scripts . . . 45
Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases . . . 46
Product Compatibility . . . 46
Hardware Compatibility . . . 46
Transceiver Compatibility for SRX Series Devices . . . 47
Finding More Information . . . 47
Documentation Feedback . . . 47
Requesting Technical Support . . . 47
Self-Help Online Tools and Resources . . . 48
Opening a Case with JTAC . . . 48
Revision History . . . 49

Introduction

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

These release notes accompany Junos OS Release 15.1X49-D60 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-D60 supports SRX300, SRX320, SRX340, SRX345, SRX550 High Memory (SRX550M), SRX1500, vSRX, and 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).

For more details about SRX Series high-end 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-D60 for the SRX Series devices.

- Release 15.1X49-D60 Software Features on page 6

Release 15.1X49-D60 Software Features

Application Layer Gateways (ALGs)

- **Express Path support on SRX5000 line devices with IOC2 and IOC3 for ALG traffic**—Starting with Junos OS Release 15.1X49-D60, SRX5400, SRX5600, and SRX5800 devices with the SRX5K-MPC (IOC2), SRX5K-MPC3-100G10G (IOC3), and SRX5K-MPC3-40G10G (IOC3) support Express Path (formerly known as services offloading) for ALG traffic.

  Express Path is a mechanism for processing fast-path packets in the Trio chipset instead of in the SPU. This method reduces the long packet-processing latency that arises when packets are forwarded from network processors to SPUs for processing and back to IOCs for transmission.

  When the IOCs have Express Path enabled and a policy with Express Path configured, Express Path qualification checks are performed right before the session is installed.

  The following ALG data traffic that supports Express Path—FTP, H.323 (only RTP/RTCP sessions are offloaded), MGCP, MS RPC, RSH, RTSP, SCCP, SIP (only RTP/RTCP sessions are offloaded), SUN RPC, TALK (only TCP sessions are offloaded), and TFTP.

  DNS, IKE and ESP, PPTP, and SQL-NET ALG data traffic do not support Express Path.

  Once an Express Path session is setup, packets cannot be sent to the SPU again.

  [See Express Path Overview and ALG Overview.]

AppSecure

- **Advanced policy-based routing (APBR) on vSRX instances and SRX Series devices**—Starting with Junos OS Release 15.1X49-D60, SRX Series Services Gateways support advanced policy-based routing (APBR) to specify the outgoing or egress interface for the traffic based on applications.

  APBR involves classifying a session based on applications and applying the configured rules to reroute the traffic. In order to classify the applications, a deep packet inspection (DPI) engine is used. The DPI engine inspects the content of a traffic session to identify the application. The result of identification is cached in application system cache (ASC). For subsequent sessions, ASC lookup is done to reroute the packet according to a matching rule.

  APBR allows you to define the routing behavior based on applications by providing more flexible traffic-handling capabilities that offer granular control for forwarding packets based on application attributes.

  [See Understanding Advanced Policy-Based Routing.]

Authentication and Access Control

- **Zone-based global user identity logging for SRX Series devices**—Starting with Junos OS Release 15.1X49-D60, the integrated user firewall feature includes support for global, zone-based user identity logging. This feature allows you to direct the system to write to the log user identity information for all users who belong to a zone if that zone is configured with the **source-identity-log** statement. The zone must be used as the source zone in a security policy that matches traffic from the users requesting access for it to take effect.

  [See *Understanding How to Include User Identity Information in the Session Log File Based on the Source Zone*.]

Class of Service

- **CoS support for the st0 interface for SRX300, SRX320, SRX340, SRX345, SRX550M devices and vSRX2.0 instances**—Starting with Junos OS 15.1X49-D60, class of service (CoS) features such as classifier, policer, queuing, scheduling, shaping, rewriting markers, and virtual channels can now be configured on the secure tunnel interface (st0) for point-to-point VPNs. The st0 tunnel interface is an internal interface that can be used by route-based VPNs to route cleartext traffics to an IPsec VPN tunnel. Table 1 on page 7 shows the different CoS features supported on SRX Series devices.

Table 1: st0 CoS Feature Support

Platform	Classifier	Policer	Queuing, Scheduling, Shaping	Rewriting Markers	Virtual Channels
Branch SRX Series devices	Supported	Supported	Supported	Supported	Supported
High-end SRX Series devices	Supported	Supported	Not supported	Supported	Not supported
vSRX2.0	Supported	Supported	Supported	Supported	Supported

NOTE: The st0 CoS features are not supported on SRX1500 devices.

Flow-based and Packet-based Processing

- **ARP request throttling** —Starting in Junos OS Release 15.1X49-D60, configuring Address Resolution Protocol (ARP) request throttling is supported on SRX5000 line devices.

  This feature allows you to bypass the previously hard-coded ARP request throttling time default (10 seconds per SPU for each IP address) and set the time to a greater value (10 through 100 seconds). Setting the throttling time to a greater value reduces the high utilization of the Routing Engine, allowing it to work more efficiently. You can configure the ARP request throttling time using the **set forwarding-options next-hop arp-throttle <*seconds*>** command.

  [See Understanding Chassis Cluster Redundancy Group IP Address Monitoring.]

- **IPv6 support for Equal-cost multipath (ECMP) flow-based forwarding on vSRX instances and SRX300, SRX320, SRX340, SRX345, SRX550M, SRX1500, SRX5400, SRX5600, and SRX5800 devices** —Starting with Junos OS Release 15.1X49-D60, IPv6 support for ECMP flow-based forwarding is available in addition to the existing IPv4 support.

  [See *Understanding ECMP Flow-Based Forwarding* topic in the Traffic Sampling, Forwarding, and Monitoring Feature Guide for Routing Devices.]

Interfaces

- **Alarm for PIC offline at start time for SRX5400, SRX5600, and SRX5800 devices**—Starting with Junos OS Release 15.1X49-D60, a new alarm is introduced to alert the conditions on the PICs (I/O card or SPC) that remain offline after the system start. A system alarm occurs when an PIC fails to come online after 40 minutes of system start time.

  [For more information, see Alarm Overview.]

- **Chassis Cluster (HA) link encryption using MAC-Sec on SRX340 and SRX345** —Starting in Junos OS Release 15.1X49-D60, Media Access Control Security (MACsec) is supported on control and fabric ports of SRX340 and SRX345 devices in chassis cluster mode.

  MACsec is an industry-standard security technology that provides secure communication for all traffic on Ethernet links. MACsec provides point-to-point security on Ethernet links between directly connected nodes and is capable of identifying and preventing most security threats, including denial of service, intrusion, man-in-the-middle, masquerading, passive wiretapping, and playback attacks. For devices in chassis cluster mode, static secure association key (SAK) and connectivity association key (CAK) are used to secure the control and fabric links.

  [See Understanding Media Access Control Security (MACsec) for SRX Series.]

J-Web

- Starting with Junos OS Release 15.1X49-D60, J-Web supports JDHCPD configuration and monitoring on all SRX Series devices.

Multicast

- **Multicast Buffer Feature support on SRX Series devices**—Starting with Junos OS Release 15.1X49-D60, dropped packets are avoided on all SRX Series devices when multicast (S, G) route resolutions are pending (up to 100 packets if buffer resources are sufficient). For example, during the creation of a single multicast session (before the session state becomes valid), multicast can handle traffic of 2000 packets per second and can queue up to 100 packets during pending (S, G) route resolves on SRX5800 devices. If multiple multicast sessions are created at the same time, then fewer packets are held (because the number of available buffers is decreased).

  [See Multicast Feature Guide for Security Devices.]

NAT

- **PAT port capacity increase, interim logging, and block recycling** —Starting with Junos OS Release 15.1X49-D60, increased PAT port capacity is supported on SRX5400, SRX5600, and SRX5800 devices with next-generation Services Processing Cards (SPCs) using the CLI option **port-scaling-enlargement**, at the [**edit security nat source**] hierarchy level.

  Interim logging and block recycling for port block allocation (PBA) are supported on all SRX Series devices using the CLI options **interim-logging-interval** and **last-block-recycle-timeout** at the [**edit security nat source pool *poolname* port block-allocation**] hierarchy level.

  [See *Network Address Translation Feature Guide for Security Devices*.]

Public Key Infrastructure

- **PKI enhancements for SRX300, SRX320, SRX340, SRX345, SRX1500, SRX5400, SRX5600, and SRX5800 devices and vSRX instances**—Starting with Junos OS 15.1X49-D60, X509 certificate management with PKI supports the following:

  - New operational commands that allow an administrator to manually initiate reenrollment of end-entity certificates with Certificate Management Protocol version 2 (CMPv2) or Simple Certificate Enrollment Protocol (SCEP). See the **request security pki local-certificate re-enroll scep** and **request security pki local-certificate re-enroll cmpv2** commands.

  - Configuration of a source IP to be used for communication with external servers for certificate enrollment and reenrollment using SCEP and CMPv2, for CRL download using HTTP and LDAP, and for Online Certificate Status Protocol (OCSP). See the **source-address** option in the [**edit security pki ca-profile *ca-profile-name***] statement. If this optional field is not specified, the IP address of the egress interface is used as the source address.

- When a secondary node joins a chassis cluster, it automatically retrieves trusted CA certificates, end-entity certificates, and key pairs from the primary node.
- Key pairs can be exported for a requested end-entity certificate using a PKCS8 envelope with the **request security pki key-pair export certificate-id *certificate-id* filename *filename*** command.
- For SNMP polls, **jnxIpSecTunnelMonTable** includes **jnxIpSecTunMonVpnName** to display the IPsec object name and **jnxIpSecTunMonTsName** to display active traffic selectors.

Sky Advanced Threat Prevention

- **Support for SRX340 and SRX345 devices** —Junos OS Release 15.1X49-D60 and later releases support Sky ATP running on the SRX340, SRX345, and SRX550M devices and vSRX instances, in addition to the existing support for SRX1500, SRX5400, SRX5600 and SRX5800 devices.

  [See the Sky Advanced Threat Prevention Supported Platforms Guide.]

VPNs

- **Dynamic VPN remote access for Secure Pulse clients to SRX300, SRX320, SRX340, SRX345, and SRX550M devices**—Starting with Junos OS Release 15.1X49-D60, dynamic VPN simplifies remote access by enabling Pulse Secure clients to establish IPsec VPN tunnels to SRX services gateways without having to manually configure VPN settings on their PCs or laptops. User authentication is supported through a RADIUS server or a local IP address pool.

  Pulse Secure client software can be downloaded from the Juniper Networks Download Software site at https://www.juniper.net/support/downloads/?p=pulse#sw; see the Pulse Secure documentation for supported client platforms.

  [See Dynamic VPN Overview for SRX services gateway information.]

- **IKEv2 reauthentication for SRX300, SRX320, SRX340, SRX345, SRX550M, SRX1500, SRX5400, SRX5600, and SRX5800 devices and vSRX instances**—Starting with Junos OS Release 15.1X49-D60, reauthentication verifies that IKEv2 VPN peers retain their access to authentication credentials. Rekeying establishes new keys for an IKE security association (SA) but does not reauthenticate the peers. Reauthentication creates a new IKE SA, creates new child SAs within the IKE SA, and then deletes the old IKE SA. IKEv2 reauthentication is disabled by default. To enable IKEv2 reauthentication, configure the **reauth-frequency** statement at the [**edit security ike policy *policy-name***] hierarchy level; the **reauth-frequency** value is the number of IKE rekeys that occurs before reauthentication occurs. For example, if **reauth-frequency** is **1**, reauthentication occurs every time there is an IKE rekey. If **reauth-frequency** is **2**, reauthentication occurs at every other IKE rekey. If **reauth-frequency** is **3**, reauthentication occurs at every third IKE rekey.

  [See Understanding IKEv2 Reauthentication.]

- **Increased IKE security associations for SRX5400 devices with two SPCs and SRX5600 and SRX5800 devices with at least three SPCs**–Starting in Junos OS

Release 15.1X49-D60, an increased number of IKE security associations can be established for AutoVPN hubs with multiple traffic selectors and the st0 interface in point-to-point mode. An SRX5400 device with two SPCs can support up to 35,000 tunnels and an SRX5600 or SRX5800 device with three or four SPCs can support up to 50,000 tunnels. We recommend using three or four SPCs in the SRX5600 and SRX5800 devices. There are no changes in configuration or functionality.

[See Understanding AutoVPN with Traffic Selectors.]

Related Documentation

- Known Behavior on page 23
- Known Issues on page 29
- Resolved Issues on page 35
- Migration, Upgrade, and Downgrade Instructions on page 43

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-D60.

Application Layer Gateway

- In Junos OS Release 15.1X49-D40 and earlier, on all SRX Series devices, the DNS ALG only recorded and forwarded the DNS packets for which the packet length exceeded the threshold value (range from 512 through 8192).

  Starting in Junos OS Release 15.1X49-D50, the DNS ALG can be configured to drop the oversized DNS packets if the length exceeds the threshold value. To enable this, you need to configure the new CLI command **set security alg dns oversize-message-drop**. If the command **set security alg dns oversize-message-drop** is not configured, the DNS ALG will only record and forward the oversized DNS packets.

AppSecure

- When you upgrade or downgrade an application signature package, an error message is displayed if there is any mismatch of application IDs (unique ID number of an application signature) between the protocol bundles and the applications associated with the IDs. This scenario occurs when AppFW and AppQoS rules are configured. An example message follows:

```
Please resolve following references and try it again [edit class-of-service
application-traffic-control rule-sets RS8 rule 1 match application junos:CCPROXY]
```

  As a workaround, disable AppFW and AppQoS rules before upgrading or downgrading an application signature package. You can reenable AppFW and AppQoS rules once the upgrade or downgrade procedure is complete.

- On SRX300, SRX320, SRX340, and SRX345 devices, AppSecure is part of Juniper Networks Secure Edge software or IPS subscription license. A separate license key is not required on your device to download and install the AppID signature database updates, or to use other AppSecure features such as AppFW, AppQoS, and AppTrack.

Authentication, Authorization and Accounting (AAA)

- Starting in Junos OS Release 12.1X47-D45, the **options no-hostname** is added to the dhcp-client configuration. You set the no-hostname if you do not want the DHCP client to send the hostname with the packets (DHCP option code 12)..
- On SRX340 and SRX345 devices, the factory-default configuration has a generic HTTP configuration. To use **ge** and **fxp0** ports as management ports, you must use the **set system services web-management http** command. The Web management HTTP and HTTPS interfaces are changed to fxp0.0 and from **ge-0/0/1.0** through **ge-0/0/7.0**.

Chassis Cluster

- **Chassis cluster initial hold timer**—Starting with Junos OS Release 15.1X49-D60, the initial hold timer is extended from 30 seconds to 120 seconds in chassis clusters on SRX340 and SRX345 devices.
- **Chassis cluster new display value**Starting in Junos OS Release 15.1X49-D60, a new field, **security**, has been added to the **show chassis cluster interfaces** command to display the status of MACsec on control and fabric interfaces.
- **Chassis cluster ineligible timer**—Starting with Junos OS Release 15.1X49-D60, the ineligible timer is 5 minutes when MACsec on the chassis cluster control port is enabled on SRX340 and SRX345 devices.
- **802.1x-protocol-daemon**—Starting with Junos OS Release 15.1X49-D60, the 802.1x protocol process (daemon) does not support restart on SRX340 and SRX345 devices.
- When an SRX Series device is operating in chassis cluster mode and encounters any IA-chip access issue in an SPC or an I/O Card (IOC), a minor FPC alarm will be activated to trigger redundancy group failover.
- Starting in Junos OS Release 15.1X49-D20, for all SRX Series devices, reth interface supports proxy ARP.

CLI

- **Discard option support with IP-monitoring**—Starting with Junos OS Release 15.1X49-D60, a new route option, **discard**, has been introduced to IP-monitoring to be able to discard a route instead.

  To enable the **discard** option, use the following CLI command:

  set services ip-monitoring policy *<policy-name>* **then preferred-route route** *<prefix>* **discard**

- Starting with Junos OS Release 15.1X49-D60, the **modem1** option has been added to the **show wireless-wan adapter** *<adapter name>* **modem** command. The **modem1** option

displays details of the integrated modems on the CBA850 3G/4G/LTE Wireless WAN Bridge.

Dynamic Host Configuration Protocol (DHCP)

- Starting with Junos OS Release 15.1X49-D60, the legacy DHCPD (DHCP daemon) configuration on all SRX Series devices is being deprecated and only the new JDHCP CLI will be supported. When you upgrade to Junos OS Release 15.1X49-D60 and later releases on a device that already has the DHCPD configuration, the following warning messages are displayed:

  WARNING: The DHCP configuration command used will be deprecated in future Junos releases.

  WARNING: Please see documentation for updated commands.

  To ensure uninterrupted service to existing user implementation of DHCP relay service, the following configuration items are identified as missing (edit and interface hierarchies) between the old DHCPD and the new JDHCPD configurations:

  ```
  set forwarding-options helpers bootp description
  set forwarding-options helpers bootp client-response-ttl
  set forwarding-options helpers bootp maximum-hop-count
  set forwarding-options helpers bootp minimum-wait-time
  set forwarding-options helpers bootp vpn
  set forwarding-options helpers bootp relay-agent-option
  set forwarding-options helpers bootp dhcp-option82
  ```

  and the interface hierarchy:

  ```
  set forwarding-options helpers bootp interface interface-name description
  set forwarding-options helpers bootp interface interface-name client-response-ttl
  set forwarding-options helpers bootp interface interface-name maximum-hop-count
  set forwarding-options helpers bootp interface interface-name minimum-wait-time
  set forwarding-options helpers bootp interface interface-name vpn
  set forwarding-options helpers bootp interface interface-name relay-agent-option
  set forwarding-options helpers bootp interface interface-name dhcp-option82
  ```

- The legacy DHCPD (DHCP daemon) will soon be deprecated. The DHCP CLI (jdhcpd process) is supported on all SRX Series devices. For more information, see https://kb.juniper.net/InfoCenter/index?page=content&id=TSB16991

Flow-based and Packet-based Processing

- **Source address for SRX5400, SRX5600, and SRX5800 devices and vSRX2.0 instances**—Starting with Junos OS 15.1X49-D60, management traffic can originate from a specific source address for Domain Name System (DNS) names.

  Consider the following when you configure the source address for DNS:

  - Only one source address can be configured as the source address for each DNS server name.

- IPv6 source addresses are supported for IPv6 DNS servers, and only IPv4 addresses are supported for IPv4 DNS servers. You cannot configure an IPv4 address for an IPv6 DNS server or an IPv6 address for an IPv4 DNS server.

To have all management traffic originate from a specific source address, configure the system name server and the source address. For example:

```
user@host# set system name-server 5.0.0.1 source-address 4.0.0.3
```

Installation and Upgrade

- Starting in Junos OS Release 15.1X49-D60, on SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices, the following factory-default configurations are changed:
  - The **name-server** statement, used to configure one or more Domain Name System (DNS) name servers, is changed to 8.8.8.8 and 8.8.4.4. Previously, it was 208.67.222.222 and 208.67.220.220.
  - A new system service, NETCONF service over SSH, is introduced at the **[edit system services]** hierarchy:

    ```
    edit system services netconf ssh
    ```

  - The following configuration setting for HTTPS (secure management) access using the J-Web interface is changed. Now, there is no need to specify the interface details for J-Web management. With this configuration, you can manage the device from any interface through HTTPS.

    ```
    edit system services web-management https interface [irb.0]
    ```

  - A license autoupdate URL (https://ae1.juniper.net/junos/key_retrieval) is now supported under the **[edit system]** hierarchy:

    ```
    license {
      autoupdate {
        url https://ae1.juniper.net/junos/key_retrieval;
      }
    }
    ```

  - A new system log configuration is introduced to configure system log messages to record all commands entered by users and all authentication or authorization attempts under the **[edit system]** hierarchy:

    ```
    syslog {
      archive size 100k files 3;
      user * {
        any emergency;
      }
      file messages {
        any notice;
        authorization info;
      }
    ```

```
    file interactive-commands {
      interactive-commands any;
    }
}
```

- Factory-default configuration—Starting with Junos OS Release 15.1X49-D50, Layer 2 Ethernet switching is not supported on the same interface for SRX300, SRX320, SRX340, SRX345, and SRX550M devices.

  The **system autoinstallation interfaces <interface names>** command and the **set interface <interface names> unit 0 family ethernet-switching** command cannot be configured on the same interface.

  NOTE: **USB auto-installation is not supported on SRX1500 devices and vSRX instances.**

  In Junos OS Release 15.1X49-D40 and earlier, configuring autoinstallation using USB and Layer Ethernet switching was supported on the same interface. However, the command caused the interface-control (dcd) process to exit, resulting in improper installation of the interface-related configurations.

- Starting in Junos OS Release 15.1X49-D50, the **request system scripts add *package-name* no-copy | unlink** command is updated to include the following options for installing AI Script install packages on SRX Series devices in a chassis cluster:

  - **master**- Install AI script packages on the primary node.
  - **backup**- Install AI script packages on the secondary node.

  This enhancement eliminates the need for separate AI script installations on the primary node and the secondary node.

Interfaces and Routing

- In Junos OS Release 15.1X49-D40 and earlier, on all SRX Series devices, GARP packets were sent out only for one IP address per IFL during RG1+ failover.

  Starting with Junos OS Release 15.1X49-D50, the IP address count per IFL during RG1+ failover has been enhanced to support up to eight IP addresses when sending GARP packets.

- **GRE keepalive time feature for SRX Series devices**—Starting in Junos OS Release 15.1X49-D30, the GRE keepalive time feature is supported on the GRE tunnel interface. You can configure the keepalives on a GRE tunnel interface using the **keepalive-time** and **hold-time** commands at the [**edit protocols oam gre-tunnel interface interface-name**] hierarchy level.

Intrusion Detection and Prevention (IDP)

- On all SRX Series devices, the following new CLI options are introduced:
  - The **checksum-validate** option has been added to the following hierarchies:

[edit security idp custom-attack ipv4_cust attack-type signature protocol ipv4]

[edit security idp custom-attack tcp_cust attack-type signature protocol tcp]

[edit security idp custom-attack udp_cust attack-type signature protocol udp]

[edit security idp custom-attack icmp_cust attack-type signature protocol icmp]

[edit security idp custom-attack icmpv6_cust attack-type signature protocol icmpv6]

To configure this option, use the following commands:

set security idp custom-attack ipv4_cust attack-type signature protocol ipv4 checksum-validate

set security idp custom-attack tcp_cust attack-type signature protocol tcp checksum-validate

set security idp custom-attack udp_cust attack-type signature protocol udp checksum-validate

set security idp custom-attack icmp_cust attack-type signature protocol icmp checksum-validate

set security idp custom-attack icmpv6_cust attack-type signature protocol icmpv6 checksum-validate

- The new **checksum-validate** option allows you to specify a particular checksum to match. The following example shows a command to validate the user-specified checksum of match equal value 0x20:

```
set security idp custom-attack ipv4_cust attack-type signature protocol ipv4
 checksum-validate match equal value 0x20
```

- The **routing-header** option and the **destination-option** option have been added to the [**edit security idp custom-attack ipv6_cust attack-type signature protocol ipv6 extension-header**] hierarchy. The **routing-header** option inspects the **routing-header** type field and reports a custom attack if a match with the specified value is found. The **destination-option** option inspects the header option type of **home-address** and **option-type** field in the extension header and reports a custom attack if a match is found.

  To configure these options, use the following commands:

  set security idp custom-attack ipv6_cust attack-type signature protocol ipv6 extension-header routing-header

  set security idp custom-attack ipv6_cust attack-type signature protocol ipv6 extension-header destination-option

  NOTE: For extension header of subtype **routing-header**, all type of inspections are supported as per RFC.

  For extension header of subtype **destination-option**, the **home-address** and the **option-type** field type of inspections are supported.

- On all SRX Series devices, the following new CLI commands are introduced:
  - The new **ihl** option at the [**edit security idp custom-attack ipv4_custom attack-type signature protocol ipv4**] hierarchy level is used to inspect the length of the IPv4 header. To configure the **ihl** option, use the following command:

    ```
    set security idp custom-attack ipv4_custom attack-type signature protocol
    ipv4 ihl
    ```

  - The new **reserved** option at the [**edit security idp custom-attack tcp_custom attack-type signature protocol tcp**] hierarchy level is used to inspect the three reserved bits in the TCP header. To configure the **reserved** option, use the following command:

    ```
    set security idp custom-attack tcp_custom attack-type signature protocol tcp
     reserved
    ```

- On SRX Series devices, starting for Junos OS Release 15.1X49-D50, a new CLI option **drop-on-syn-in-window** is introduced for controlling the IDP behavior when SYN is seen in the TCP window. To enable this option use the **set security idp sensor-configuration re-assembler drop-on-syn-in-window** command.

  When the **sensor-configuration** option is:

  - Disabled (Not set (default))—Drops the packet and ignore current session.
  - Enabled (Set)—Drops the packet after IDS processing is complete.

Junos OS XML API and Scripting

- Starting with Junos OS Release 15.1X49-D60, the REST API is supported on SRX300, SRX320, SRX340, SRX345, SRX550M, SRX5400, SRX5600, and SRX5800 devices.

J-Web

- J-Web supports only the new CLI configurations. For more information, see https://kb.juniper.net/InfoCenter/index?page=content&id=TSB16991

Layer 2 Features

- **LLDP and LLDP-MED for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices**—Starting with Junos OS Release 15.1X49-D60, Link Layer Discovery Protocol (LLDP) and LLDP-Media Endpoint Discovery (MED) are enabled on SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.

  Starting with Junos OS Release 15.1X49-D70, Link Layer Discovery Protocol (LLDP) and LLDP-Media Endpoint Discovery (MED) are supported on Layer 3 interfaces for SRX300, SRX345, SRX550M, and SRX1500 devices.

- **IRB logical interface statistics**—Starting with Junos OS Release 15.1X49-D60, interface statistics are supported on the IRB logical interface for SRX300, SRX320, SRX340, SRX345, and SRX550M devices.

To verify the IRB logical interface statistics, enter the **show interfaces irb.<index> extensive** and **show interfaces irb.<index>statistics** commands.

- **Global MAC limit**—Starting with Junos OS Release 15.1X49-D60, the maximum number of MAC addresses learned on all logical interfaces on the SRX1500 device is 24,575. When this limit is reached, incoming packets with a new source MAC address will be dropped.
- Starting in Junos OS Release 15.1X49-D50, the factory-default configuration of the SRX300, SRX320, SRX340, and SRX345 devices is switching mode. When these devices are loaded or reset with the factory-default configuration, they start up in switching mode.
- **Enhanced Layer 2 CLI**—Starting with Junos OS Release 15.1X49-D10, enhanced Layer 2 CLI configurations are supported on SRX5400, SRX5600, and SRX5800 devices. Legacy Layer 2 transparent mode configuration statements and operational commands are not supported. If you enter legacy configurations in the CLI, the system displays an error and fails to commit the configurations.

  For example, the following configurations are no longer supported:

  - **set bridge-domain**
  - **set interfaces ge-1/0/0 unit 0 family bridge**
  - **set vlans vlan-1 routing-interface**

  Use the SRX L2 Conversion Tool to convert Layer 2 CLI configurations to enhanced Layer 2 CLI configurations.

  The SRX L2 Conversion Tool is available at https://www.juniper.net/support/downloads/?p=srx5400#sw .

  For more information, refer to the Knowledge Base article at https://kb.juniper.net .

  [See Enhanced Layer 2 CLI Configuration Statement and Command Changes.]

MPLS

- Starting in Junos OS Release 15.1X49-D50, the **vrf-table-label** statement allows mapping of the inner label to a specific Virtual Routing and Forwarding (VRF). This mapping allows examination of the encapsulated IP header at an egress VPN router. For SRX Series devices, the **vrf-table-label** statement is currently supported only on physical interfaces. As a workaround, deactivate **vrf-table-label** or use physical interfaces.

Multicast

- Starting with Junos OS Release 15.1X49-D40, for all SRX Series devices, configuration of patterns in standard PCRE format is supported in the custom attacks.

NAT

- Starting with Junos OS Release 15.1X49-D60, when you delete or modify a NAT rule, a NAT pool, or an interface address, the related NAT bindings might not be deleted

immediately. In addition, the related session scan for the NAT rule and NAT pool might not be deleted as quickly as in previous releases.

- In Junos OS Release 15.1X49-D45 and earlier, on SRX Series devices and in vSRX instances, the system log messages in IDP attack logs contained only IPv4-based NAT address fields.

  Starting in Junos OS Release 15.1X49-D50, the system log messages in IDP attack logs contain both IPv4-based and IPv6-based NAT address fields.

- Source NAT pool port configuration options—Starting with Junos OS Release 15.1X49-D40, the **port-overloading-factor** option and the **port-range** option at the [edit security nat source pool *source-pool-name* port] hierarchy level can be configured together. Prior to Release 15.1X49-D40, the options would overwrite each other.

  [See *port (Security Source NAT)*]

Network Time Protocol

- Starting in Junos OS Release 15.1X49-D10, on all SRX Series devices, when the NTP client or server is enabled in the [**edit system ntp**] hierarchy, the REQ_MON_GETLIST and REQ_MON_GETLIST_1 control messages supported by the monlist feature within the NTP client or server might allow remote attackers, causing a denial of service. To identify the attack, apply a firewall filter and configure the router's loopback address to allow only trusted addresses and networks.

Public Key Infrastructure

- The **request security pki local-certificate enroll** command now includes the **cmpv2** and **scep** keywords for CMPv2 and SCEP certificate enrollment. Each keyword has configurable options. In previous releases, SCEP enrollment parameters were entered after the **enroll** keyword. Starting with this release, SCEP enrollment parameters should be entered after the **scep** keyword. In a future release, SCEP enrollment parameters after the **enroll** keyword will be deprecated.

  The **auto-re-enrollment** configuration statement at the [**edit security pki**] hierarchy level now includes the **cmpv2** and **scep** keywords for automatic reenrollment of local certificates using CMPv2 or SCEP. Each keyword has configurable options. In previous releases, SCEP enrollment parameters were entered after the **set security pki auto-re-enrollment certificate-id** *certificate-id-name* statement. Starting with this release, SCEP reenrollment parameters should be entered after the **scep** keyword. In a future release, SCEP enrollment parameters after the **set security pki auto-re-enrollment certificate-id** *certificate-id-name* statement will be deprecated.

Screen

- In Junos OS releases earlier than Junos OS Release 15.1X49-D20, the firewall generates a log for every packet that exceeds the source-ip-based or destination-ip-based threshold and triggers the source or destination session limit. This can lead to a flood of logs if a large number of packets is received every second after the threshold has been reached. For example, if the source or destination session limit has been reached and 100 additional packets arrive in the next second, 100 log messages are sent to the system log server.

  Starting in Junos OS Release 15.1X49-D20, the firewall generates only one log message every second irrespective of the number of packets that trigger the source or destination session limit.

  This behavior also applies to flood protection screens with TCP-Synflood-src-based, TCP-Synflood-dst-based, and UDP flood protection.

System Logs

- In Junos OS Release 15.1X49-D30 and earlier, the severity parameter for RT_SRC_NAT_PBA messages was “debug”.

  Starting in Junos OS Release 15.1X49-D40, the severity parameter has changed. The RT_SRC_NAT_PBA messages are now fixed with severity as “info”.

  The following example shows RT_SRC_NAT_PBA messages before Junos OS Release 15.1X49-D40:

  16:32:43.760393 In IP (tos 0x0, ttl 254, id 16957, offset 0, flags [none], proto: UDP (17), length: 218) 192.0.2.4.syslog > 192.0.2.2.syslog: SYSLOG, length: 190 Facility user (1), Severity debug (7)

  Feb 5 16:32:49 RT_NAT: RT_SRC_NAT_PBA_ALLOC: Subscriber 192.0.2.2 used/maximum [1/32] blocks, allocates port block [27200-27263] from 198.51.100.3 in source pool src-nat-pool-1 lsys_id: 0\012

  The following example shows RT_SRC_NAT_PBA messages in Junos OS Release 15.1X49-D40, indicating the change in the severity parameter:

  16:32:43.760393 In IP (tos 0x0, ttl 254, id 16957, offset 0, flags [none], proto: UDP (17), length: 218) 192.0.2.4.syslog > 192.0.2.2.syslog: SYSLOG, length: 190 Facility user (1), Severity info (6)

  Feb 5 16:32:49 RT_NAT: RT_SRC_NAT_PBA_ALLOC: Subscriber 192.0.2.2 used/maximum [1/32] blocks, allocates port block [27200-27263] from 198.51.100.3 in source pool src-nat-pool-1 lsys_id: 0\012

System Management

- During a load override, to enhance the memory for the commit script, you must load the configuration by applying the following commands before the commit step:
  set system scripts commit max-datasize 800000000
  set system scripts op max-datasize 800000000
- On all SRX Series devices in transparent mode, packet flooding is enabled by default. If you have manually disabled packet flooding with the **set security flow ethernet-switching no-packet-flooding** command, then multicast packets such as OSPFv3 hello packets are dropped.

Unified Threat Management (UTM)

- Starting with Junos OS Release 15.1X49-D60, on SRX1500 Services Gateways and vSRX instances, UTM policies, profiles, MIME patterns, filename extensions, and protocol-command numbers are increased to 500; custom URL patterns and custom URL categories are increased to 1000.
- In Junos OS Release 15.1X49-D45 and earlier, the structured log of Web filtering has inappropriate field names.

  Starting in Junos OS Release 15.1X49-D50, the structured log fields have changed. The corresponding fields in the UTM Web filter logs WEBFILTER_URL_BLOCKED, WEBFILTER_URL_REDIRECTED, and WEBFILTER_URL_PERMITTED are now fixed with the appropriate structured log fields.

The following example shows WEBFILTER_URL_BLOCKED messages before Junos OS Release 15.1X49-D50:

<12>1 2016-02-18T01:32:50.391Z utm-srx550-b RT_UTM - WEBFILTER_URL_BLOCKED [junos@2636.1.1.1.2.86 source-address="192.0.2.3" source-port="58071" destination-address="198.51.100.2" destination-port="80" name="cat1" error-message="BY_BLACK_LIST" profile-name="uf1" object-name="www.example.com" pathname="/" username="N/A" roles="N/A"] WebFilter: ACTION="URL Blocked "192.0.2.3(58071)->198.51.100.2(80) CATEGORY="cat1" REASON="BY_BLACK_LIST" PROFILE="uf1" URL=www.example.com OBJ=/ username N/A roles N/A

The following example shows WEBFILTER_URL_BLOCKED messages in Junos OS Release 15.1X49-D50, indicating the change in structured log fields:

<12>1 2016-02-18T01:32:50.391Z utm-srx550-b RT_UTM - WEBFILTER_URL_BLOCKED [junos@2636.1.1.1.2.86 source-address="192.0.2.3" source-port="58071" destination-address="198.51.100.2" destination-port="80" category="cat1" reason="BY_BLACK_LIST" profile="uf1" url="www.example.com" obj="/" username="N/A" roles="N/A"] WebFilter: ACTION="URL Blocked" 192.0.2.3(58071)->198.51.100.2(80) CATEGORY="cat1" REASON="BY_BLACK_LIST" PROFILE="uf1" URL=www.example.com OBJ=/ username N/A roles N/A

The structured log field changes in the UTM Web filter logs WEBFILTER_URL_BLOCKED, WEBFILTER_URL_REDIRECTED, and WEBFILTER_URL_PERMITTED are as follows:

- **name -> category**
- **error-message -> reason**
- **profile-name -> profile**
- **object-name -> url**
- **pathname -> obj**

User Interface and Configuration

- You can configure only one rewrite rule for one logical interface. When you configure multiple rewrite rules for one logical interface, an error message is displayed and the commit fails.

VPNs

- The **show security dynamic-vpn client version** command is not supported for dynamic VPN.

Zones and Interfaces

- System services configuration option—Starting with Junos OS Release 15.1X49-D40, the **system-services** option at the **[edit security zones security-zone *zone-name* host-inbound-traffic]** hierarchy level and the **system-services** option at the **[edit security zones security-zone *zone-name* interfaces *interface-name* host-inbound-traffic]** hierarchy level no longer support the configuration of the Session Initiation protocol (SIP) system service.

  [See *system-services (Security Zones Interfaces)* and *system-services (Security Zones Host Inbound Traffic)*.]

Related Documentation

- New and Changed Features on page 5
- Known Behavior on page 23
- Resolved Issues on page 35
- Known Issues on page 29
- Migration, Upgrade, and Downgrade Instructions on page 43

Known Behavior

This section contains the known behaviors, system maximums, and limitations in hardware and software in Junos OS Release 15.1X49-D60.

AppSecure

- When you delete or disable a custom application signature, and the configuration commit fails, the application system cache (ASC) entry is not cleared completely; instead, a base application in the path of custom application will be reported in ASC.
- On SRX Series devices, when you change the timeout value for the application system cache entries using the command **set services application-identification application-system-cache-timeout**, the cache entries need to be cleared to avoid inconsistency in timeout values of existing entries.

Attack Detection and Prevention (ADP)

- On all high-end SRX Series devices, the first path signature screen is performed first, followed by the fast path bad-inner-header screen.
- On all SRX Series devices, when a packet allow or drop session is established, the bad-inner-header screen is performed on every packet, because this screen is a fast path screen.

CLI

- On SRX5000 line devices, the following CLI statement is deprecated—rather than immediately removed—to provide backward compatibility and a chance to bring your configuration into compliance with the new configuration:

  set chassis fpc <*fpc-slot*> services offload

  The following new CLI statement replaces the deprecated CLI statement:

  set chassis fpc <*fpc-slot*> np-cache

Class of Service

The following limitations apply to CoS support on VPN st0 interfaces:

- Currently, the maximum number for software queues is 2048. If the number of st0 interfaces exceeds 2048, not enough software queues can be created for all the st0 interfaces.
- Shaping threshold depends on two factors: interface bandwidth and shaping rate. Every interface bandwidth is received from its parent physical interface, which is divided by shaping and scheduling at the logical interface. Currently, the st0 physical interface is a pseudointerface and its maximum bandwidth is 622.08 Mbps, meaning that all of the IPsec tunnel throughput cannot exceed 622 Mbps. You must ensure that the shaping rate that you configure is smaller than its physical egress traffic.
- Only route-based VPN can apply st0 CoS. Table 2 on page 24 describes the st0 CoS feature support for different types of VPN.

Table 2: CoS Feature Support for VPN

Classifier Features	Site-to-Site VPN (P2P)	ADVPN/AutoVPN (P2MP)
Classifiers, policers, and rewriting markers	Supported	Supported
Queueing, scheduling, and shaping based on st0 logical interfaces	Supported	Not supported
Queueing, scheduling, and shaping based on virtual channels	Supported	Supported

- On branch SRX Series devices, one st0 logical interface can bind to multiple VPN tunnels. The eight queues for the st0 logical interface cannot reroute the traffic to different tunnels, so pre-tunneling is not supported.

  NOTE: The virtual channel feature can be used as a workaround on branch SRX Series devices.

- When defining a CoS shaping rate on an st0 tunnel interface, consider the following restrictions:
  - The shaping rate on the tunnel interface must be less than that of the physical egress interface.
  - The shaping rate only measures the packet size that includes the inner Layer 3 cleartext packet with an ESP/AH header and an outer IP header encapsulation. The outer Layer 2 encapsulation added by the physical interface is not factored into the shaping rate measurement.
  - The CoS behavior works as expected when the physical interface carries the shaped GRE or IP-IP tunnel traffic only. If the physical interface carries other traffic, thereby lowering the available bandwidth for tunnel interface traffic, the CoS features do not work as expected.
- On SRX550M, SRX5400, SRX5600, and SRX5800 devices, bandwidth limit and burst size limit values in a policer configuration are a per-SPU, not per-systerm limitation. This is the same policer behavior as on the physical interface.

Flow-based and Packet-based Processing

- On SRX340 and SRX345 devices, fabric interfaces must be configured such that the Media Access Control Security (MACsec) configurations are local to the nodes. Otherwise, the fabric link will not be reachable.
- You can configure a security master password that allows you to encrypt shared secrets, such as RADIUS passwords and IKE preshared keys. Having a master password allows devices to encrypt passwords in such a way that only devices running Junos OS that have knowledge of the master password can decrypt the encrypted passwords. The following limitations apply:
  - The master password cannot be edited, deleted, or modified in the config-private mode.
  - For security reasons, the **deactivate system master-password** option is not supported.
  - Rolling back to a previous configuration that used a different master password is not allowed.
- On SRX Series devices, the default mode for processing traffic is flow mode. To configure an SRX Series device as a border router, you must change the mode from flow-based processing to packet-based processing. Use the **set security forwarding-options family mpls mode packet-based** statement to configure the SRX device to packet mode. You must reboot the device for the configuration to take effect.

General Packet Radio Service (GPRS)

- Starting in Junos OS Release 15.1X49-D40, the SCTP flow session utilizes a connection tag to more finely distribute SCTP traffic across SPUs on SRX5400, SRX5600, and SRX5800 devices that support the SCTP ALG. The connection tag is decoded from the SCTP vtag. A separate SCTP session will be created for each of the first three packets—that is, one session for INIT, INIT-ACK, and COOKIE-ECHO, respectively. Because, the reverse-direction traffic has its own session, the session can no longer match the existing forward-direction session and pass through automatically. Therefore, similar to the forward-direction policy, an explicit policy is needed for approving the reverse-direction SCTP traffic. In this scenario, the SCTP flow session requires a bidirectional policy configuration to be established for even a basic connection.
- On SRX5000 line devices, when you use the GTP inspection feature, during an ISSU from Junos OS Release 15.1X49-D10, 15.1X49-D20, or 15.1X49-D30 to Junos OS Release 15.1X49-D40 or later, GTPv0 tunnels will not be synchronized to the upgraded node.

  For GTPv1 and GTPv2, the tunnels will be synchronized, but the timeout gets restarted.

  Beginning with Junos OS Release 15.1X49-D40, ISSU is fully supported with the GTP inspection feature enabled.

Integrated User Firewall

- For integrated user firewall in Junos OS 151.X49-D50 you cannot use the Primary Group, whether by its default name of Domain Users or any other name (if you happened to have changed it), in integrated user firewall configurations.

  When a new user is created in Active Directory, the user is added to the global security group Primary Group which is by default called Domain Users. The Primary Group is less specific than other groups created in Active Directory because all users belong to it. Consequently it can become very large.

IP Monitoring

- On SRX5400, SRX5600, and SRX5800 devices, IP monitoring does not support MIC online/offline status.

Layer 2 Features

- **Layer 2 Bridging and Transparent Mode**— On all SRX Series devices, bridging and transparent mode are not supported on Mini-Physical Interface Modules (Mini-PIMs).
- In Junos OS Release 15.1X49-D40, the following features are not supported on SRX Series devices and vSRX instances:
  - Layer 2 transparent mode policer
  - Three-color policer

Multicast

- On all SRX Series devices, only 100 packets can be queued during pending (S, G) route. However, when multiple multicast sessions enter the route resolve process at the same time, buffer resources are not sufficient to queue 100 packets for each session.
- On all SRX Series devices, when a multicast route is not available, pending sessions are not torn down, and subsequent packets are queued. If no multicast route resolve comes back, then the traffic flow has to wait for the pending session to timed out. Then packets can trigger new pending session create and route resolve.

Platform and Infrastructure

- On all high-end SRX Series devices, when you enable a global services offloading policy utilizing IOC2 line-cards, the connections per second (CPS) rate might be reduced. It is recommended to utilize IOC3 line-cards to maximize the CPS rate, or alternatively, lower the session count to ensure that the IOC2 is capable of scaling. As a workaround, identify the sessions that must be offloaded and only enable services offloading on those sessions.

Software Installation and Upgrade

- On SRX5000 Series devices, In-Service Software Upgrade (ISSU) is not supported for upgrading from earlier Junos OS releases to Junos OS Release 15.1X49. ISSU is supported for upgrading to successive Junos OS Release 15.1X49 releases and to major Junos OS releases.

  NOTE: **SRX300 Series devices, SRX550M, and SRX1500 devices do not support ISSU.**

USB autoinstallation

- On SRX300 Series Services Gateways on which the USB auto-installation feature is enabled (the default configuration), removal of a USB storage device immediately after insertion is not supported.

  NOTE: **USB auto-installation is not supported on SRX1500 devices.**

  After you insert a USB storage device, Junos OS scans the device to check whether it contains the USB autoinstallation file. This process might take up to 50 seconds to complete depending on the quality of the USB storage device and the number and size of the files in the device. Removing the USB storage device while this process is running might cause the services gateway to reboot, the USB port to stop working, and data loss on the USB. We recommend that after inserting a USB storage device, you wait for at least 60 seconds before removing it.

  By issuing the **set system autoinstallation usb disable** command (which disables the USB autoinstallation feature) before you insert the USB device, you can reduce the waiting interval between insertion and removal of a USB storage device from 60 seconds to 20 seconds.

VPN

- On SRX Series devices, configuring RIP demand circuits over P2MP VPN interfaces is not supported.
- On high-end SRX Series devices, do not use ISSU if upgrading from Junos OS Release 15.1X49-D30 through Junos OS Release 15.1X49-D60, if using any VPN configurations.

As a workaround deactivate or remove all the VPN commands from the configuration before executing ISSU. If the workaround is used, all VPN tunnels and VPN traffic will be dropped during ISSU upgrade. Once ISSU has completed you may then re-enable the VPNs as before.

Related Documentation

- New and Changed Features on page 5
- Changes in Behavior and Syntax on page 11
- Known Issues on page 29
- Resolved Issues on page 35
- Migration, Upgrade, and Downgrade Instructions on page 43

Known Issues

This section lists the known issues in hardware and software in Junos OS Release 15.1X49-D60.

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

Chassis Clustering

- On high-end SRX Series devices in a chassis cluster, after reboot if the secondary node (RG1) claim cold synchronize (CS) completes first, this might result in bidirectional RTO synchronization or incorrect direction for RTO synchronization. PR1138502
- On high-end SRX Series devices, when large configuration with 32 logical systems and more than 10,000 NAT rules is load override by one without logical system and NAT, the NSD might core on the backup node occasionally. The chassis cluster can be set up normally after the crash. PR1183342

Command-Line Interface (CLI)

- On SRX Series devices running Junos OS Release 15.1X49-D50, the **master-password** parameter such as **iteration-count** and **pseudorandom-function** configuration cannot take effect after the configuration is committed. The user has to configure the **master-password** plain-text-password again to make the parameter changing take effect. PR1179095
- On devices running Junos OS Release 15.1X49-D50, a higher master-password iteration count (such as 1000) with large scale shared secret configuration (10000 and more) might impact the configuration commit time even though the configuration change is minor and has nothing to do with the shared secret. PR1181000

Dynamic Host Configuration Protocol (DHCP)

- On SRX1500 devices, after you commit the DHCPv6 configuration, the DHCPv6 relay might not work, because the reply packet is dropped. PR1142727

Flow-based and Packet-based Processing

- On high-end SRX Series devices, when a device forwards traffic, a flowd core file is generated. This is a generic issue and does not impact any feature. PR1027306
- On SRX Series devices, default trusted-ca list (Trusted_CAs.pem) is not bundled with Junos. PR1044944
- On SRX550M with 2G memory devices, traffic processed by the serialization process is dropped when the maximum limit of serialization sessions (32,000) is exceeded. As a result, advanced services such as IDP, ALG, GTP, SCTP, and AppSecure are impacted. The limitation of max serialization sessions should be enlarged to 64000. PR1061524
- On branch SRX Series devices, the maximum-sessions value is not displayed correctly. PR1094721
- On high-end SRX Series devices, in central point architecture, syslog is sent out per second per SPU. Hence, the number of SPUs define the number of syslog per second. PR1126885
- On SRX1500 devices, the log buffer size is expanded to 30,000 in event mode. When the log buffer size was 1000, the Packet Forwarding Engine generated logs burst when there were more than 30 entries and more logs were dropped. PR1133757
- On SRX Series devices in chassis cluster, if you want to use J-Web to configure and commit some of 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, the security intelligence block-drop action for C and C policy for custom_url_data feed does not work. PR1141745
- On SRX1500 devices, when CPU goes very high (95%+), there is possibility that the connection between AAMW daemon and PKID daemon can be broken. In this case, the AAMW daemon will keep being in Initializing state until that connection is established. PR1142380
- On SRX1500 devices, after the user changes the revocation configuration of a CA profile, the change cannot be populated to the SSL-I's revocation check. It is recommended to change SSL-I configuration to enable or disable CRL checking instead of ca-profile configuration. PR1143462
- On SRX1500 devices in a chassis cluster with 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 high-end SRX Series devices, if revocation-check is enabled in a CA-profile that does not have CRL information present, then Packet Forwarding Engine (PFE) might stop working. PR1144836

- On high-end SRX Series devices with SRX5K-MPC (IOC2) cards installed and np-cache feature enabled, low performance might be seen when fragmented traffic is present. PR1193769
- On SRX3400, SRX3600, SRX5400, and SRX5600 devices, the BGP might flap if using reth interface to establish BGP neighbors and the control link and the fabric link might flap at the same time. As a result, the traffic which is traversing it will be interrupted. PR1194548

Interfaces

- On branch SRX Series devices, DHCP on VDSL interface is flapping. IP address to this interface will lead to interface down, then trigger DHCP will remove the IP, after interface is UP, DHCP re-assigning the IP to this interface will cause interface down again, which causes a dead loop.

  As a workaround, set a hold up time that will keep interface up during VDSL negotiation with peer. Doing this will avoid this DHCP dead loop. The hold up time value must be larger than the VDSL link set up time. example **set interfaces pt-4/0/0 hold-time up 60000 down 60000**. PR1131243
- On SRX1500 devices, when 1G SFP-T is used on the 1G SFP ports (ge-0/0/12 to ge-0/0/15), it does not come up at 100M speed PR1133384
- On SRX Series devices, source MAC filtering does not work on trunk ports. PR1143994

J-Web

- Branch SRX Series devices, do not have dedicated management and control port. HA wizard for SRX300 line devices use ge-0/0/3 as management port to access J-Web post HA configuration. Working with ge-0/0/3 mandates you to be near the device (possible to access device in switched private network also) and automatically configures a private IP to the interface ge-0/0/3. It also configure SRX device as a DHCP Server which assigns an IP to the connected device from the same subnet to which this interface belongs.

  There is very thin line on this implementations of HA configuration Wizard for SRX300 line devices and SRX550M. If you unknowingly make the secondary device up the J-Web will get stuck at that point and further configuration like fab port or some optional configurations would get missed out and the complete HA configuration will not work.

  As a workaround, follow the configuration wizard strictly. When the wizard prompts you to make the secondary device up then make the secondary device up. PR1142955
- Error messages are seen on J-Web when adding a custom-applications setting with "term". As a workaround, setting the same in CLI works fine or setting the UUID in J-Web works fine, however, UUID is not a mandatory option. PR1183037
- On SRX Series devices, J-Web **Chassis Viewer** should be stable and should not drag.

  To avoid the this:

  - Do not drag and drop the chassis viewer image within the pages, this will lead to misalignment in the dashboard.

- Avoid minimizing any browser while using J-Web, this will lead to usability issues like scroll bar will be missed and you cannot view the full screen.

  As a workaround:

  - Navigate to other tabs like Configure, Monitor and return back to dashboard to get the proper view.
  - Maximize the browser and refresh the page.

  PR1204481

- On branch SRX Series devices, you cannot launch setup wizard after pressing reset configuration button when the device is in L2 Transparent mode. You can launch the setup wizard by pressing reset configuration button on the device when the device is in switching mode. As a workaround, reboot the device after pressing the reset configuration button when the device is in L2 Transparent mode. PR1206189
- On SRX1500 devices in J-Web there is no support for the Snapshot functionality **Maintain->Snapshot->Target Media->Disk ->Click Snap Shot** as this functionality is not supported on the device. PR1204587
- On SRX Series devices, as part of JDHCP changes DHCP relay configuration under **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, As part of JDHCP changes DHCP client bindings under **Monitor** is removed for Junos OS Release 15.1X49-D60. The same bindings can be seen in CLI using the **show dhcp client binding** CLI command. PR1205915

Layer 2 Ethernet Services

- On SRX Series devices configured as a DHCP server (using the jdhcpd process), when the DHCP server gets a new request from a client and applies an IP address from the authentication process (authd), the jdhcpd process communicates with authd twice as expected (once for the DHCP discovery message and once for the DHCP request message). If the authentication fails in the first message, the authd process will indefinitely wait for the second authentication request. However, the jdhcpd process never sends the second request, because the process detects that the first authentication did not occur. This causes memory leak on the authd process, and the memory might get exhausted, generating a core file and preventing DHCP server service. High CPU usage on the Routing Engine might also be observed. PR1042818
- On SRX1500 devices configured in Ethernet switching mode, few MAC entries are shown in 'show ethernet-switching table' even after MAC age out time. This issue is applicable only when SRX1500 MAC learning table has more than 17K MACs. PR1194667

Network Address Translation (NAT)

- On high-end SRX Series devices, security policies are not downloaded after ISSU from Junos OS Release 12.1X46-D40 to Junos OS Release 12.1X46-D45, 12.3X48-D10 or higher, when NAT is configured. PR112095

- On all high-end SRX Series devices, security policies are not downloaded after ISSU from Junos OS Release 12.1X46-D40 to Junos OS Release 12.1X46-D45, 12.3X48-D10 or higher, when NAT is configured. PR1120951
- On SRX Series devices, intranet IPs can communicate with each other on open ports when you use only "junos-persistent-nat" application in trust-to-trust policy with persistent NAT and Hairpin. This issue can be avoided when "destination-address drop-untranslated" is configured in the policy. PR1171160

Network Management and Monitoring

- On high-end SRX devices, **set system time-zone** configuration does not affect time stamp in stream mode security log. PR1203833

Platform and Infrastructure

- On SRX3000 line devices, when a USB flash device with a mounted filesystem is physically detached by a user. Currently, the system may panic in this situation. This is a known Freebsd issue which is resolved in version 7.3 and later. PR695780
- On SRX210 or SRX220 chassis cluster, if a VLAN interface is configured as the interface of JDHCP server, then the DHCPDISCOVER message will be dropped on the switch chip, which results in the function of JDHCP server failure. PR1088134
- On high-end SRX Series devices, if global SOF policy (all session service-offload) is enabled, the connections per second (CPS) will be impacted due to IOC2 limitation. It is recommended to use IOC3 card if many sessions need to be SOF or lower the SOF session amount to make sure IOC2 is capable of handling it. PR1121262
- On high-end SRX Series devices, if system service rest API is added to the configuration, though commit can be completed, all the configuration change in this commit will not be able to take effect. This is caused due to the rest-api daemon failing to come up as the interface IP is not available during bootup. The configuration is not read on the Routing Engine side. PR1123304
- On SRX Series devices, File Descriptor (FD) might leak on the httpd-gk process when system fails to connect to the mgd process management socket. PR1127512
- On branch SRX Series devices, on addition or deletion of VLANs, the DHCP address will not be acquired by the client and fails from the JDHCP server. As a workaround, restart dhcp-services on the client. PR1139495
- On all high-end SRX devices, flowd process might crash and cause traffic outage if the SPU (Services Processing Unit) CPU usage is higher than 80%. Therefore, some threads are in waiting status and the watchdog cannot be toggled timely causing the flowd process to crash. PR1162221
- On high-end SRX Series devices, configuration synchronization fails when IPsec Internal SA over control link is enabled. As a workaround, disable the internal-sa feature.PR1162964

Routing Policy and Firewall Filters

- On high-end SRX Series devices, if there are two routing instances of instance type default and virtual router, when you change the instance type of one routing instance from default to virtual router after the routing policy is configured, the route is missing from the second routing instance. PR969944
- On SRX5800 devices in a chassis cluster, the flowd process would crash after a reboot with IPv6 security policies configured. PR1089272
- On all SRX Series devices, there might be a traffic outage if failover happens between node0 and node1 and the network security daemon (NSD) fails to read the security policies from the configuration file. As a workaround, restart the NSD until you recover NSD using the **restart network-security** command. PR1182591

System Logs

- On SRX Series devices, many **help syslog** messages are missing in Junos OS Release 12.1X44 and later releases. PR1159910

Unified Threat Management (UTM)

- On SRX Series devices, when the size of an attachment is larger than 20 MB, the SMTP antivirus scanning of UTM fails to transfer the attached file. PR838503
- On high-end SRX Series devices, under high CPS and UTM SAV interested traffic, SRX might ramp up to 99% CPU usage due to central lock of object cache memory allocation. There is no clear boundary since allocation race condition is varying. Basically, reducing traffic CPS could lower high CPU usage. PR967739
- On branch SRX Series devices (especially SRX550M) with Sophos Antivirus (SAV) configured, some files whose sizes are larger than the max-content-size might not go into fallback. Instead, some protocols do not predeclare the content size. PR1005086

VPNs

- On SRX Series devices, if IPsec VPN tunnel is established using IKEv2, few drops might be observed during CHILD_SA rekey with the reason "bad SPI", when the SRX is the responder for this rekey. PR1129903
- On branch SRX Series devices, customer using IKEv2 and agressive mode for several gateways, where the external interfaces are the same, after some time of establishment, when trying to renew phase one, logs will show that the VPN will try to use the information of the last established VPN to renew this one, leading to a failure to reestablished the IPsec VPN. PR1187988
- On branch SRX Series devices with chassis cluster enabled, when the RG0 failover occurs, the pp0 interface will flap if the IPsec VPN tunnel is established using a pp0 interface as the external interface. Due to a timing issue, the pp0 interface flapping might cause the VPN tunnel session and IPsec Security Association (SA) installed in

the data-plane to be deleted but the IKE/IPsec SA installed in the Routing Engine will remain causing the VPN traffic outage. PR1143955

- On branch SRX Series devices, when using P2MP IPSec VPN tunnels with Dynamic routing over tunnel, a ksyncd core may be encountered after RG0 failover on previous RG0 primary node, if dynamic routing is removed from VPN tunnel prior to RG0 failover. PR1170531

Related Documentation

- New and Changed Features on page 5
- Changes in Behavior and Syntax on page 11
- Known Behavior on page 23
- Resolved Issues on page 35
- Migration, Upgrade, and Downgrade Instructions on page 43

Resolved Issues

This section lists the issues fixed in hardware and software in Junos OS Release 15.1X49-D60.

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

Resolved Issues

Application Layer Gateways (ALGs)

- On branch SRX Series devices, the flowd process crashes and generates a core dump while processing MS-RPC or SUN-RPC traffic on the secondary node. PR1190929
- On SRX Series devices, MSRPC ALG cannot decrypt encrypted EPM messages (authlevel RPC_C_AUTHN_LEVEL_PKT_PRIVACY) and drops the encrypted EPM messages. New behavior will be to bypass such encrypted messages and generate a syslog message. PR1192477
- On high-end SRX Series devices, the flowd core might crash on node1 and causes the ISSU failure while performing ISSU from 12.1X44-D60.2 to 12.1X46-D55.1 or above 12.1X46 build. PR1193679
- On all SRX platforms, when RSH ALG is enabled by manually, RSH ALG receives a message whose stderr port is 0, RSH ALG will drop packets and will not open gate for it. When encounter the issue, please disable RSH ALG. PR1196530

Authentication and Access Control

- On SRX Series devices, in the environment of pass-through firewall user authentication, a warning message will be generated while committing the configuration pass-through firewall user authentication. PR1166723
- On SRX Series devices, when configuring the application-identification service applications, the tab completion feature does not work. PR1180707
- On SRX Series devices, authentication source's should not have same priority. PR1184494
- On SRX Series devices, during HTTP and HTTPS pass-through firewall authentication, the device incorrectly removes preceding colon in the password string. This causes the authentication to fail and the authentication entry cannot be created in case there is preceding colon in password string. PR1187162

Chassis Cluster

- On high-end SRX Series devices in HA mode, dhcp server lost the information about the clients after fail over. But the pool information is not lost, so the clients can get new addresses from the server. The issue only happens once during the failover. PR1097132
- On high-end SRX Series devices, when two GTP-U packets have the same address and different TEID and if these two packets are assigned to same SPU to process, the flow session for the secondary packet cannot be setup. PR1182920
- The flowd daemon on the primary node of an SRX Series chassis cluster may crash and restart when attempting to synchronize a multicast session created via crafted multicast packets. Upon the flowd crash, data plane redundancy groups will fail over to the secondary node in the chassis cluster while flowd on the primary node restarts. Refer to JSA10768 for more information. PR1188853
- On branch SRX Series devices, in the chassis cluster, the fabric link flaps randomly after upgrading to the 12.1X46 and onwards. PR1197954
- On all SRX Series devices with dual fabric link chassis cluster, one of fabric link sometimes shows as down after RG0 failover or node reboot even there is fabric probe on the link. PR1207919

Flow-based and Packet-based Processing

- On SRX5400, SRX5600, and SRX5800 devices, the buffer for advanced security services (ALGs, UTM, AppSecure, etc) might be exhausted by heavy application traffic (e.g., heavy DNS traffic processed by DNS ALG causes exhausted buffer), which will impact all advanced security services, and causes the related application traffic outage. The buffer is enlarged for SPC II to mitigate the impact by the fix. PR1177189
- On all SRX Series devices, when configuring white-list for Security Screen, it might cause memory corruption in Jtree, which results in the flowd process crash. PR1172844

- On SRX240, SRX340, SRX345, SRX550, and SRX650 platforms, the interface might not work under promiscuous mode even flexiable-ethernet-service is configured. This issue occurs occasionally. PR1176484
- On SRX High-end platforms with chassis cluster enabled, under heavy traffic load the primary cluster node may experience a flowd coredump while the secondary node is booting up. PR1177853
- On all high-end SRX devices, traffic is affected when the traffic open connection is from two directions at the same time. Configure a bidirectional traffic permit policy to avoid this issue. PR1178954
- On devices running Junos OS Release 15.1X49-D50, the master-password parameter (such as iteration-count and pseudorandom-function) configuration cannot take effect after the configuration is committed. The user has to configure the master-password plain-text-password again to make the parameter changing take effect. PR1179095
- On all SRX chassis clusters, IPsec VPN traffic will be dropped intermittently if Jflow is enabled and sends out packets to remote server through an IPsec VPN tunnel via st0 interface. This is because few Jflow packets will be sent out by the backup node and causes ESP sequence number out of order. PR1180537
- On all high-end SRX devices, SRX does not send out icmp type 3 code 4 packet if it works in HA cluster and the SPC card is in the combo mode. By default, all high-end SRX Series devices are in the combo mode, as per the perspective of the SPC (Services Processing Card), which means that the SPC acts as both the CP SPU and FLOW SPU PR1183249
- On SRX Series devices, in Layer 2 and Layer 3 mixed-mode, with flooding enabled, when there is no Layer 2 egress interface up, a packet from Layer 2 interface might be forwarded to Layer 3 interface wrongly during the flooding process. PR1189004
- On high-end SRX devices with appqos enabled, some of sessions hit appqos policy will not be created properly at high memory utilization. As a result, packet related the session will drop. PR1190889
- On SRX300 series devices, the **request system software** command with the **partition** option fails with the following error **ERROR: Could not determine the internal media for srx3xx**. PR1192353
- On SRX5400 and SRX5600 devices, when issuing the **show security flow session summary** command, the bfd sessions might flap PR1198266
- Prior to Junos OS Release 15.1X49-D60 all formats in ISO8601 such as "2016-06-06T00:31:52-07:00" are not supported. Now this format is supported for the query communication with Aruba server. PR1198521
- On SRX300 line devices in chassisd file, the following messages are logged, **Cannot read hw.chassis.startup_time: No such file or directory**. PR1202367

- On SRX Branch devices and SRX1500, in Junos 15.1X49-D40 and 15.1X49-D50, SCTP traffic does not pass through the device because the reverse session wing does not install correctly and the INIT-ACK is dropped. PR1204177
- On the SRX300 line devices, system autorecovery stops working when USB storage is disabled. PR1207964

Infrastructure

- On all SRX Series devices with health monitor configured for Routing Engine, the system health management process (syshmd) might crash due to a memory corruption in some rare conditions, such as in the scenario that concurrent conflicting manipulation of the file system occurs. PR1069868
- When you plug out and re-plug the modem at CBA750B/CBA850, leading to CBA750B/CBA850 MIB tree change. This might cause the SRX Series device to not get the modem information from the expected MIB node. In such scenarios, the device will display the following modem information: "Connection status: Down" and all counters are set to zero by default. This is a status show problem, data link may still work. To fix this problem, just reboot the CBA750B/CBA850. CBA750B/CBA850 will rebuild the MIB tree and SRX Series device can get the information correctly. PR1187675

Interfaces

- On branch SRX Series devices, front panel HA Indicator shows incorrect LED status when you run the **show chassis craft-interface node 0/1** command. PR1189006
- On SRX1500 with 15.1X49, the IPsec packets terminating on a VLAN tagged interface are corrupted with a duplicate 16 byte packet header. PR1177119
- On branch SRX Series devices, interface statistics are not supported on the IRB interface. PR1182205
- On SRX300 series platforms, when configuring loopback option on a physical interface, it does not work. PR1184229
- On SRX Series devices , if the bootp flag is (0x0000) unicast, host can not get IP address from dhcp server which on IRB interface PR1184905
- On SRX1500 devices, when a SFP (SRX-SFP-1GE-SX) transceiver is plugged into a SFP port, it works well. However, when it is plugged into a SFP+ ports, it shows as UNSUPPORTED. PR1191710
- On branch SRX Series devices, panic reboot on node1 after commit interface pp0 - panic: Assertion cont_info != NULL (file ../../../../../../../src/junos/bsd/sys/netpfe/rt_pfe_nh_container.c, line 4346) failed. PR1193661
- On SRX1500 XE ports, enabling and disabling autoneg using **gigether-option auto-negotiation** configuration brings down the port. PR1196398

Intrusion Detection and Prevention (IDP)

- On all SRX-branch series platform, which is using hardware DFA instead of PCRE for IDP policy matching with 1G memory constraint, the secondary node might fail to sync and be in disabled status. PR1167673
- On SRX Series devices, you cannot compile the IDP policy when lsys idp-policy-combined is created. PR1187731

J-Web

- On SRX Series devices, when Web Auth is in use BAD_PAGE_FAULT will be seen when you try to login to the web-auth page. PR1180787

Layer 2 Features

- On branch SRX Series devices, on Layer 2 - learning switching mode with vlan-id 1 configured, ARP is not learnt correctly. PR1190969
- On SRX1500 devices, when LACP is configured, rebooting the device can trigger 'l2ald' core sometimes. PR1202370
- LLDP-MED is supported on SRX300, SRX320, SRX320-POE, SRX340, SRX345, and SRX550M devices starting from Junos OS Release 15.1X49-D60 PR1202689

Network Address Translation (NAT)

- On all SRX Series devices, when vSRX or SRX is doing NAT66, the ICMPv6 packet will has a wrong TCP sequence after NAT66. This might cause the client side to not accept the ICMPv6 packet, so that the service cannot connect. This issue affects all types of ICMPv6 error messages. PR1183188
- On high-end SRX Series devices, the Network Security Daemon (NSD) may crash on backup node occasionally if a large configuration with 32 logical-systems and more than 10000 NAT rules are loaded and overrided by a configuration without logical system and NAT. The chassis cluster can be set up normally after the crash. PR1183342
- While using Source based NAT with egress interface translation, upon egress interface IP address change, current NAT sessions may not be removed until session is aged-out. Traffic loss will be encountered while traffic attempts to pass on sessions using old egress interface NAT IP. PR1201415

Network Management and Monitoring

- On all high-end SRX devices in chassis cluster, when there are both IPv4 and IPv6 traffic processed by the device, due to a timing issue in session manipulation (session installation and deletion) by multiple real-time threads, the flow entry might be leaked in the flow table. This issue might cause the flowd process crash on the backup node. PR1180162
- On all high-end SRX devices, when you run show system license usage command it may show invalid scale-subscriber license on new RG0 master node after RG0 failover.

This is only a cosmetic issue and there is no impact to function/performance/traffic. PR1197211

Platform and Infrastructure

- On all high-end SRX devices in a chassis cluster with dual control links, if the first control link (em0) goes down, the master Routing Engine does not send the IP traffic to the remote node. This means that if, for example, redundancy group 0 (control plane) is primary on one node and redundancy group 1 (data plane) is primary on another node, any IP traffic originated on the Routing Engine will not be passed out. PR1051535
- On SRX5000 line devices, when control link is down, the secondary node becomes ineligible and then goes to disabled state. But FPCs restart continuously after going to disabled state when they should remain offline till rebooted. PR1170024
- On SRX1500 devices, after applying the command **request system zeroize** command and restoring the device to factory default, adding minimal required config to have ssh management to the device, the SSH does not work. PR1184162
- On SRX Series devices, one or multiple J-Web sessions are established in the browser. After navigating different tab and multiple PHP processes are remained. This cause high CPU usage on RE. When encountering the issue, please use the workaround to restore it. PR1186172
- On SRX Series devices, vulnerability in IPv6 processing has been discovered that may allow a specially crafted IPv6 Neighbor Discovery (ND) packet to be accepted by the router rather than discarded. The crafted packet, destined to the router, will then be processed by the routing engine (RE). A malicious network-based packet flood, sourced from beyond the local broadcast domain, can cause the RE CPU to spike, or cause the DDoS protection ARP protocol group policer to engage. When this happens, the DDoS policer may start dropping legitimate IPv6 neighbors as legitimate ND times out. Refer to JSA10749 for more information. PR1191838
- On SRX Series devices, with pass-through authentication, FWclient access destination server by old browser(browser like MS-IE4/MS-IE5), the flowd process might crash when pass-through http traffic matches the fwauth-policy. PR1203294

Routing Policy and Firewall Filters

- On all SRX Series devices, when range-address is configured on an address-book and invoked by a security policy, an abnormal memory access might occur, which causes the flowd process crash. PR1196122

User Interface and Configuration

- On branch SRX Series devices, after rolling back (rollback 0) and loading override configuration continuously, the system will eventually fail to commit any new configuration changes. PR1137944

Unified Threat Management (UTM)

- On SRX Series devices, , after using the UTM services, anti-virus or anti-spam for some time, DNS lookups might start to fail and the UTM service resorts to fallback. PR1207651

VPNs

- On SRX Series devices, in some cases, a memory leak might occur when using route-based or policy-based VPN and peer attempting multiple phase 2 connections with different proxy IDs. PR1174974

Related Documentation

- New and Changed Features on page 5
- Changes in Behavior and Syntax on page 11
- Known Behavior on page 23
- Known Issues on page 29
- Migration, Upgrade, and Downgrade Instructions on page 43

Documentation Updates

This section lists the errata and changes in the software documentation.

- Starting in Junos OS Release 15.1X49-D60, content from the *Junos OS CLI User Guide* is available in Junos OS 15.1 CLI User Guide. On the 15.1X49-D60 page, click **CLI User Guide** to view information about the Junos OS command-line interface.

  This guide does not indicate SRX Series device support in the Supported Platforms list and other related support information; however, the Junos OS features described in the Junos OS 15.1 *CLI User Guide* are supported on SRX Series devices. For full, confirmed support information about SRX Series devices, refer to Feature Explorer.

- Starting in Junos OS Release 15.1X49-D60, content from the *Junos OS Installation and Upgrade Guide for Security Devices* is available in the *Junos OS 15.1 Installation and Upgrade Guide*. On the 15.1X49-D60 page, click **Installation and Upgrade** to view installation and upgrade information.

This guide does not indicate SRX Series device support in the Supported Platforms list and other related support information. However, the Junos OS features described in the Junos OS 15.1 *Installation and Upgrade Guide* are supported on SRX Series devices. For full, confirmed support information about SRX Series devices, refer to Feature Explorer.

- Starting in Junos OS Release 15.1X49-D60, content from the *Network Monitoring and Troubleshooting Guide for Security Devices* is available in the Network Management Administration Guide for Routing Devices. On the 15.1X49-D60 page, click **Network Monitoring and Troubleshooting** to view the *Junos OS 15.1 Network Management Administration Guide for Routing Devices*.

  This guide does not indicate SRX Series device support in the Supported Platforms list and other related support information. However, the Junos OS features described in the Junos OS 15.1 *Network Management Administration Guide for Routing Devices* are supported on SRX Series devices. For full, confirmed support information about SRX Series devices, refer to Feature Explorer.

- Starting in Junos OS Release 15.1X49-D60, the *Multicast Feature Guide for Security Devices* is available in *15.1 Multicast Protocols Feature Guide for Routing Devices*. On the 15.1X49-D60 page, click **Multicast** to view information on multicast concepts and configuration examples.

  This guide does not indicate SRX Series device support in the Supported Platforms list and other related support information. However, the Junos OS features described in the Junos OS 15.1 *Multicast Protocols Feature Guide for Routing Devices* are supported on SRX Series devices. For full, confirmed support information about SRX Series devices, refer to Feature Explorer.

- Starting in Junos OS Release 15.1X49-D60, content from the Junos OS *Routing Protocols Library for Security Devices* is available in the *15.1 Junos OS Routing Protocols Library for Routing Devices*. On the 15.1X49-D60 page, click **Routing Protocols** to view general routing protocol concepts and configuration information, including information about multitopology routing, interior gateway protocols (IS-IS, OSPF, RIP), and BGP.

  This guide does not indicate SRX Series device support in the Supported Platforms list and other related support information. However, the Junos OS features described in the Junos OS 15.1 *Junos OS Routing Protocols Library for Routing Devices* are supported on SRX Series devices. For full, confirmed support information about SRX Series devices, refer to Feature Explorer.

- Starting in Junos OS Release 15.1X49-D60, information about MIBs is available in SNMP MIBS Explorer. On the 15.1X49-D60 page, click **SNMP MIB Explorer** to view MIBs information. Use the MIBs Explorer to search for and view information about various MIBs, MIB objects, and SNMP notifications that are supported on Juniper Networks devices.

- Starting in Junos OS Release 15.1X49-D60, content from the *Junos OS Standards Reference*, APIs, and scripting guides are available in *15.1 Standards Reference* and API and Scripting section of Junos OS Release 15.1 page. On the 15.1X49-D60 page, click **Standards Reference** or **APIs and Scripting** to view information about standards and APIs and scripting, respectively.

The Junos OS 15.1 *Standard Reference* does not indicate SRX Series device support in the Supported Platforms list and other related support information. However, the Junos OS features described in this guide are supported on SRX Series devices. For full, confirmed support information about SRX Series devices, refer to Feature Explorer.

- Starting in Junos OS Release 15.1X49-D60, information about system log messages is available in System Log Explorer. On the 15.1X49-D60 page, click **System Log Explorer** to view system log information. Use the System Log Explorer to search for and view information about various system log messages.

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 for Layer 2 Configuration on page 43
- Upgrade and Downgrade Scripts for Address Book Configuration on page 43

Upgrade for Layer 2 Configuration

Starting with Junos OS Release 15.1X49-D10 and later, only enhanced Layer 2 CLI configurations are supported. If your device was configured earlier for Layer 2 transparent mode, then you must convert the legacy configurations to Layer 2 next-generation CLI configurations.

For details on how to migrate from Junos OS Release 12.3X48-D10 and earlier releases to Junos OS Release 15.1X49-D10 and later releases, refer to the Knowledge Base article at https://kb.juniper.net/InfoCenter/index?page=content&id=KB30445.

Upgrade and Downgrade Scripts for Address Book Configuration

Beginning with Junos OS Release 12.1, you can configure address books under the **[security]** hierarchy and attach security zones to them (zone-attached configuration). In Junos OS Release 11.1 and earlier, address books were defined under the **[security zones]** hierarchy (zone-defined configuration).

You can either define all address books under the **[security]** hierarchy in a zone-attached configuration format or under the **[security zones]** hierarchy in a zone-defined configuration format; the CLI displays an error and fails to commit the configuration if you configure both configuration formats on one system.

Juniper Networks provides Junos operation scripts that allow you to work in either of the address book configuration formats (see Figure 1 on page 45).

- About Upgrade and Downgrade Scripts on page 44
- Running Upgrade and Downgrade Scripts on page 45
- Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases on page 46

About Upgrade and Downgrade Scripts

After downloading Junos OS Release 12.1, you have the following options for configuring the address book feature:

- **Use the default address book configuration**—You can configure address books using the zone-defined configuration format, which is available by default. For information on how to configure zone-defined address books, see the Junos OS Release 11.1 documentation.
- **Use the upgrade script**—You can run the upgrade script available on the Juniper Networks support site to configure address books using the new zone-attached configuration format. When upgrading, the system uses the zone names to create address books. For example, addresses in the trust zone are created in an address book named **trust-address-book** and are attached to the trust zone. IP prefixes used in NAT rules remain unaffected.

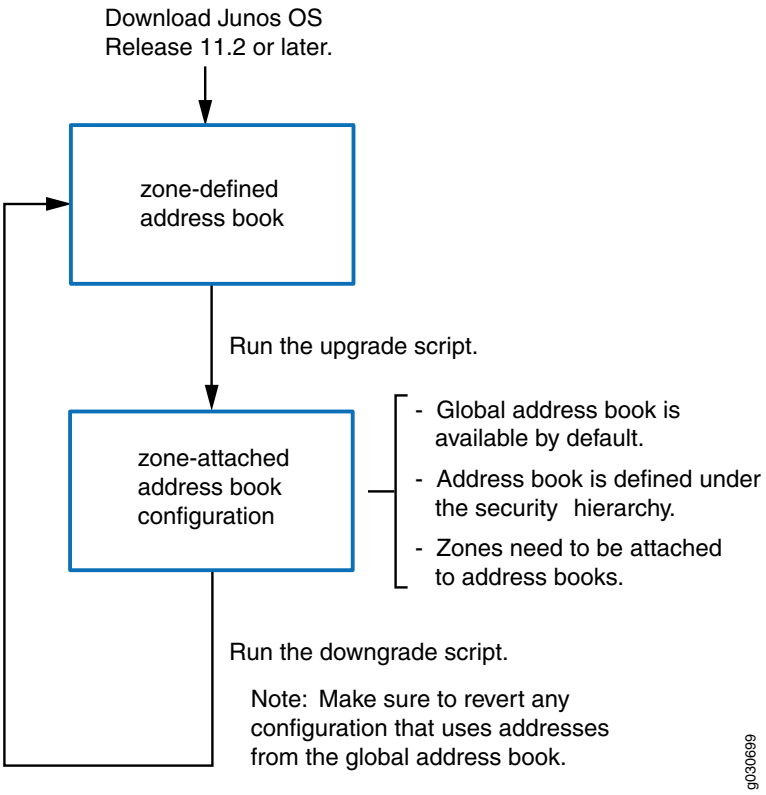
  After upgrading to the zone-attached address book configuration:

  - You cannot configure address books using the zone-defined address book configuration format; the CLI displays an error and fails to commit.
  - You cannot configure address books using the J-Web interface.

  For information on how to configure zone-attached address books, see the Junos OS Release 12.1 documentation.
- **Use the downgrade script**—After upgrading to the zone-attached configuration, if you want to revert to the zone-defined configuration, use the downgrade script available on the Juniper Networks support site. For information on how to configure zone-defined address books, see the Junos OS Release 11.1 documentation.

NOTE: Before running the downgrade script, make sure to revert any configuration that uses addresses from the global address book.

Figure 1: Upgrade and Downgrade Scripts for Address Books



Running Upgrade and Downgrade Scripts

The following restrictions apply to the address book upgrade and downgrade scripts:

- The scripts cannot run unless the configuration on your system has been committed. Thus, if the zone-defined address book and zone-attached address book configurations are present on your system at the same time, the scripts will not run.
- The scripts cannot run when the global address book exists on your system.
- If you upgrade your device to Junos OS Release 12.1 and configure logical systems, the master logical system retains any previously configured zone-defined address book configuration. The master administrator can run the address book upgrade script to convert the existing zone-defined configuration to the zone-attached configuration. The upgrade script converts all zone-defined configurations in the master logical system and user logical systems.

NOTE: You cannot run the downgrade script on logical systems.

For information about implementing and executing Junos operation scripts, see the *Junos OS Configuration and Operations Automation Guide*.

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 12.1X44, 12.1X46, and 12.3X48 are EEOL releases. You can upgrade from Junos OS Release 12.1X44 to Release 12.1X46 or even from Junos OS Release 12.1X44 to Release 12.3X48. 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.

Related Documentation

- New and Changed Features on page 5
- Changes in Behavior and Syntax on page 11
- Known Behavior on page 23
- Known Issues on page 29
- Resolved Issues on page 35

Product Compatibility

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

- Hardware Compatibility on page 46
- Transceiver Compatibility for SRX Series Devices on page 47

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

13 March 2019—Revision 6— Junos OS 15.1X49-D60 – SRX Series.

12, July 2018—Revision 5— Junos OS 15.1X49-D60 – SRX Series.

23, January 2017—Revision 4— Junos OS 15.1X49-D60 – SRX Series.

06, October 2016—Revision 3— Junos OS 15.1X49-D60 – SRX Series.

28, September 2016—Revision 2— Junos OS 15.1X49-D60 – SRX Series.

19, September 2016—Revision 1— Junos OS 15.1X49-D60 – SRX Series.