Release Notes: Junos® OS Release 15.1X49-D80 for the SRX Series

Release 15.1X49-D80
30 May 2017
Revision 4

Contents

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-D80 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/techpubs/software/junos/.

NOTE: Junos OS Release 15.1X49-D80 supports the following devices: SRX300, SRX320, SRX340, SRX345, and SRX550 High Memory (SRX550M), SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, and SRX5800 devices with host subsystems composed of either an SRX5K-RE-1800X4 (RE2) with an SRX5K-SCBE (SCB2), or an SRX5K-RE-1800X4 (RE2) with an SRX5K-SCB3 (SCB3), and vSRX.

For more details about SRX 5400, SRX5600, and SRX5800 devices hardware and software compatibility, please see http://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-D80 for the SRX Series devices.

Release 15.1X49-D80 Software Features

AppSecure

- **SSL Forward Proxy URL category policy for SRX340, SRX345, SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800 devices and vSRX instances**—Starting with Junos OS Release 15.1X49-D80, the whitelisting feature is extended to include URL categories supported by Enhanced Web filtering in the whitelist configuration of SSL forward proxy. In this implementation, the Server Name Indication (SNI) field is extracted by the UTM module from client hello messages to determine the URL category. Each URL category has a unique ID. The list of URL categories under whitelist is parsed and the corresponding category IDs are pushed to the Packet Forwarding Engine for each SSL forward proxy profile.

  [See AppSecure Services Feature Guide for Security Devices.]

- **SSL Proxy for Server Protection for SRX Series devices**—SSL proxy is a transparent proxy that performs SSL encryption and decryption between the client and the server. Starting in Junos OS Release 15.1X49-D80, the proxy model implementation for server protection (often called *reverse proxy*) is based on existing SSL plug-ins to provide improved handshaking and support for more protocol versions.

  [See Configuring Reverse Proxy.]

Chassis Cluster

- **ISSU support for SRX4100 and 4200 devices**—Starting with Junos OS Release 15.1X49-D80, SRX4100 and SRX4200 devices support in-service software upgrade (ISSU).

  ISSU enables a software upgrade from one Junos OS version to a later Junos OS version with little or no downtime. The *chassis cluster ISSU* feature enables both devices in a cluster to be upgraded from supported Junos OS versions with minimal disruption in traffic and no disruption in service.

  ISSU provides the following benefits:

  - Eliminates network downtime during software image upgrades
  - Reduces operating costs, while delivering higher service levels
  - Allows fast implementation of new features

  [See Understanding the Low-Impact ISSU Process on Devices in a Chassis Cluster.]

- **J-Flow version 9 support for SRX1500, SRX4100, SRX4200, and vSRX instances in a chassis cluster**—Starting with 15.1X49-D80, on SRX1500, SRX4100, SRX4200, and

vSRX instances, J-Flow version 9 is supported on a chassis cluster. Use of J-Flow version 9 enables you to define a flow record template suitable for IPv4 and IPv6 traffic.

[See Chassis Cluster Supported Features.]

Class of Service (CoS)

- **Non-strict-priority scheduling support for SRX300, SRX320, SRX340, SRX345, SRX550M, SRX1500 devices and vSRX instances**—On SRX Series devices, if all queue priorities send more bandwidth than the egress interface bandwidth, higher priority queues can starve lower priority queues. To prevent this, starting with Junos OS Release 15.1X49-D80, you can apply the **non-strict-priority-scheduling** option at the **[edit-class-of-service]** hierarchy level, which balances the **transmit-rate** configurations across queue priorities.

  [See non-strict-priority-scheduling.]

Ethernet Switching

- **Connectivity Fault Management (CFM) support for SRX1500 devices**—Starting in Junos OS Release 15.1X49-D80, Ethernet switching supports Ethernet OAM CFM in switching mode.

  The CFM features can be configured on GE, XE, VDSL, and Point-to-Point Protocol over Ethernet (PPPoE) interfaces. The CFM supports fault monitoring, path discovery, fault isolation and performance measurement functionalities.

  NOTE: To enable CFM on an Ethernet interface, you must configure maintenance domains, maintenance associations, and maintenance association end points (MEPs).

  [See Understanding Ethernet OAM Connectivity Fault Management .]

- **LACP support for SRX300, SRX320, SRX340, SRX345, SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, and SRX5800 devices and vSRX instances**—Starting with Junos OS Release 15.1X49-D80, LACP is supported in Layer 2 transparent mode in addition to the existing support in Layer 3 mode.

  When a device uses LACP to bundle the member links, it creates high-speed connections, known as a fat pipe, with peer systems. You can increase bandwidth by adding member links. LACP provides automatic determination, configuration, and monitoring of member links.

  LACP automatically binds member links, thereby avoiding errors that are possible when the LAG is configured manually.

  [See Understanding Link Aggregation Control Protocol.]

- **Layer 2 802.1X authentication for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices**—Starting with Junos OS Release 15.1X49-D80, Layer 2 802.1X authentication feature in switching mode is supported.

802.1X is an IEEE standard for port-based network access control (PNAC). 802.1X is part of the IEEE 802 group of protocols. 802.1X authentication provides a mechanism to authenticate devices or users attached to a LAN port.

The three basic components of a network with 802.1X are the authenticator PAE (port access entity), the supplicant, and the authentication server.

Configuring 802.1X authentication using J-Web is not supported in this release.

NOTE: **On SRX1500 devices, dynamic filters in association with dot1x is not supported. Also, radius server configuration is not supported with dot1x configurations. Hence, you cannot configure the filter ID in radius server.**

[See Understanding 802.1X Port-Based Network Authentication].

- **Multiple VLAN Registration Protocol (MVRP) support for SRX1500 device**— Starting in Junos OS Release 15.1X49-D80, the following Layer 2 features are supported in switching mode:
  - MVRP is a Layer 2 application protocol that manages dynamic VLAN registration in switching networks. The use of MVRP also manages the addition, deletion, and renaming of active VLANs, thereby reducing network administrators' time spent on these tasks.
  - Switching mode comprises of two parameters, **allowed-mac** and **shutdown-action**.

  [See Configuring Multiple VLAN Registration Protocol (MVRP) to Manage Dynamic VLAN Registration.]

- **VLAN retagging and Q-in-Q Tunneling support for SRX1500 devices**—Starting with Junos OS Release 15.1X49-D80, VLAN retagging and Q-in-Q, in switching mode is supported.

  VLAN retagging works on IEEE standard 802.1Q virtual LAN tagging (VLAN tagging). It is a part of the IEEE 802 group of protocols. The VLAN identifier in packets arriving on a Layer 2 trunk port can be rewritten or retagged with a different internal VLAN identifier.

  Q-in-Q is an Ethernet networking IEEE standard, formally known as IEEE 802.1ad. It is also known as provider bridging, stacked VLANs, or simply Q-in-Q. Q-in-Q allows multiple VLAN tags to be inserted into a single frame, an essential capability for implementing datacenter bridging network.

  [See Understanding VLAN Retagging and Understanding Q-in-Q Tunneling and VLAN Translation.]

General Packet Radio Service (GPRS)

- **GTP and SCTP ALG support for SRX1500 devices**—Starting in Junos OS Release 15.1X49-D80, the GTP and SCTP ALGs are supported on SRX1500 devices. GTP is used to transfer mobile data in the mobility core network and SCTP is widely used in a mobility network for signaling message transmissions.

  [See General Packet Radio Service Feature Guide for Security Devices.]

J-Web

- In Junos OS Release 15.1X49-D80, J-Web supports the addition of the following parameters on the existing JUNOS OS CLI for security platforms:

  1. MAC Interface limit support and LACP support in Layer 2 Transparent Mode for SRX300, SRX320, SRX340, SRX345, SRX550M, SRX1500, SRX4100, SRX4200, and vSRX devices.
  2. The Interfaces > Link Aggregation menu in J-Web is enabled for Layer 2 Transparent Mode of J-Web for the SRX300, SRX320, SRX340, SRX345, SRX550M, SRX1500, SRX4100, SRX4200, and vSRX devices.
  3. Changes in Remote Access VPN and IPsec VPN configuration.
  4. Changes to add *Non-Strict-Priority scheduling* for SRX1500 device.

Unified Threat Management (UTM)

- **E-Mail Attachments for SRX Series devices**—Starting in Junos OS Release 15.1X49-D80, e-mail management for SMTP lets enrolled SRX Series devices transparently submit potentially malicious e-mail attachments to the cloud for inspection. Once an attachment is evaluated, Sky ATP assigns the file a threat score from 0 through 10 with 10 being the most malicious. In addition, e-mails are checked against administrator-configured blacklists and whitelists. If an e-mail matches the blacklist, it is considered to be malicious and is handled the same way as an e-mail with a malicious attachment.

  [See Email Management Overview.]

- **SNI support for Web filtering for SRX Series devices**—In Junos OS Release 12.3X48-D45 and 15.1X49-D80, Junos OS supports Server Name Indication (SNI) for local, Websense-redirect, and Enhanced Web Filtering (EWF). SNI is an extension of SSL/TLS protocol to indicate what server name the client is contacting over an HTTPS connection. SNI inserts the actual hostname of the destination server in client's hello message in clear text format before the SSL handshake is complete. Web filtering uses the SNI information for further processing or modifying the query. In this implementation, the SNI includes only the server name, and not the full URL of the server.

  [See UTM Feature Guide for Security Devices.]

User Access and Authentication

- **Trusted Platform Module (TPM) to Bind Secrets for SRX300, SRX320, SRX340, and SRX345 devices**—Starting with Junos OS Release 15.1X49-D80, a software layer is added to enable the TPM's capability.

  TPM is used to protect the private keys stored in Junos, when the TPM is activated. For example, IPsec or SSL inspection uses these private keys.

  [See Using Trusted Platform Module to Bind Secrets on SRX Series Devices.]

VPNs

- **IKEv2 message fragmentation for SRX300, SRX320, SRX340, SRX345, SRX550M, SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, and SRX5800 devices and vSRX instances**—Starting in Junos OS Release 15.1X49-D80, large IKEv2 messages (such as authentication exchanges that contain multiple certificates) are fragmented; each message fragment is encrypted and authenticated before being transmitted. On the receiver, the message fragments are verified, decrypted, and merged into the original message. Message fragmentation, as described in RFC 7383, *Internet Key Exchange Protocol Version 2 (IKEv2) Message Fragmentation*, allows IKEv2 to operate in environments where IP fragments might be blocked and VPN peers would not be able to establish an IPsec security association. IKEv2 message fragmentation is enabled by default on SRX Series devices for IPv4 and IPv6 messages. You can disable fragmentation and, optionally, configure the maximum message size with the **fragmentation** statement at the [**edit security ike gateway *gateway-name***] hierarchy level.

  [See Understanding IKEv2 Fragmentation.]

- **IPv6 support for dynamic endpoint VPNs for SRX300, SRX320, SRX340, SRX345, SRX550M, SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, and SRX5800 devices and vSRX instances**—Starting with Junos OS Release 15.1X49-D80, dynamic endpoint VPNs on SRX Series devices support IPv6 traffic on secure tunnels using IKEv1 or IKEv2. The IPv6 dynamic endpoint gateway can use PKI certificates or preshared keys for authentication. A dynamic endpoint VPN is used when the remote site-to-site peer has a dynamically assigned IP address.

  NOTE: IPv6 traffic is not supported for AutoVPN networks.

  [See Understanding IPsec VPNs with Dynamic Endpoints.]

- **NCP Exclusive Remote Access Client connections to IPsec VPN gateways on SRX300, SRX320, SRX340, SRX345, SRX550M, SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, and SRX5800 devices and vSRX instances**—Starting in Junos OS Release 15.1X49-D80, SRX Series devices support IKEv1 or IKEv2 IPsec VPN connections from users running third-party NCP Exclusive Remote Access Client on Windows and MAC OS devices. NCP Exclusive Remote Access Client software can be downloaded from https://www.ncp-e.com/ncp-exclusive-remote-access-client/.

A two-user license is supplied by default on SRX Series devices; a license must be purchased and installed for additional users. The SRX Series devices use AutoVPN in point-to-point interface mode. Traffic selectors configured on the SRX Series device and the NCP client determine the client traffic to be encrypted. For IKEv1 client authentication, Extended Authentication (XAuth) is used with a RADIUS server or a local access profile. IKEv2 clients use EAP with a RADIUS server for authentication.

[See Understanding IPsec VPNs with NCP Exclusive Remote Access Client.]

- **Suite B and PRIME cryptographic suites for SRX4100 and SRX4200 devices**—Starting in Junos OS Release 15.1X49-D80, Suite B and PRIME cryptographic suites are supported on SRX4100 and SRX4200 devices. Suite B is a set of cryptographic algorithms designated by the U.S. National Security Agency to allow commercial products to protect traffic that is classified at secret or top secret levels. Protocol Requirements for IP Modular Encryption (PRIME) is an IPsec profile defined for public sector networks in the United Kingdom. It is based on the Suite B cryptographic suite but uses Advanced Encryption Standard–Galois/Counter Mode (AES-GCM) rather than Advanced Encryption Standard–Cipher Block Chaining (AES-CBC) for IKEv2 negotiations.

  [See Understanding Suite B and PRIME Cryptographic Suites.]

- **Support for SSL remote access VPNs by encapsulating IPsec traffic over TCP connections on SRX300, SRX320, SRX340, SRX345, SRX550M, SRX1500, SRX4100, and SRX4200 devices and vSRX instances**—Starting in Junos OS Release 15.1X49-D80, SRX Series devices support SSL VPN connections from users running third-party NCP Exclusive Remote Access Client on Windows and MAC OS devices. In many public hotspot environments, UDP traffic is blocked while TCP connections are allowed. To support these environments, SRX Series devices can encapsulate IPsec messages within a TCP connection. This implementation is compatible with the NCP Exclusive Remote Access Client, which can be downloaded from https://www.ncp-e.com/ncp-exclusive-remote-access-client/. A two-user license is supplied by default on SRX Series devices; a license must be purchased and installed for additional users.

  [See Understanding SSL Remote Access VPNs with NCP Exclusive Remote Access Client.]

Related Documentation

- Migration, Upgrade, and Downgrade Instructions on page 30
- Changes in Behavior and Syntax on page 9
- Known Behavior on page 14
- Known Issues on page 19
- Resolved Issues on page 24

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-D80.

Authentication, Authorization and Accounting (AAA)

- Starting with Junos OS 15.1X49-D80, the **wins-server** option at the [**edit access profile** ***profile-name***] hierarchy level allows you to configure the IPv4 address of a Windows Internet Name Service (WINS) server.

CLI

- 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-D80, a new command, **force-discover**, is introduced to the DHCP client to force the DHCP client to send a DHCP discover packet after one to three failed **dhcp-request** attempts. The **force-discover** option ensures that the DHCP server will assign the same or a new IP address to the client. To ensure that this process does not fail in the event of a DHCP server outage, the **retransmission-attempt** value has been extended from a maximum of 6 to 50,000 attempts. No changes are made to the current default values.

  To start the new DHCP process, include the **force-discover** command in the [edit interfaces] hierarchy level. For example,

  set interfaces ge-0/0/0 unit 0 family inet dhcp-client force-discover

- 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

Ethernet Switching

- **VLAN Range for SRX300, SRX320, SRX340, SRX345, and SRX550M devices**—Starting with Junos OS Release 15.1X49-D75, the VLAN range is from 1 to 4094 on inet interfaces and the VLAN range is from 1 to 3967 on Ethernet switching interfaces. On Ethernet switching interfaces, VLAN range from 3968 to 4094 falls under the reserved VLAN address range, and the user is not allowed to configure VLANs in this range.

Flow-based and Packet-based Processing

- **Source address for SRX5400, SRX5600, and SRX5800 devices and vSRX 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

Network Address Translation (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.

Public Key Infrastructure

- Generating a public key infrastructure (PKI) signature of 512 bits for a digital certificate with Digital Signal Algorithm (DSA) or RSA encryption is being deprecated on SRX Series devices and vSRX instances:

  - Starting with Junos OS Release 15.1X49-D75, the **size 512** option is not supported in the CLI command **request security pki generate-key-pair certificate-id *certificate-id-name* type dsa**. Instead, the **size** must be **1024** (the default value), **2048**, or **4096**.

  - The **size 512** option is being deprecated in the CLI command **request security pki generate-key-pair certificate-id** *certificate-id-name* **type rsa** and will no longer be supported in a future release. Instead, the **size** must be **1024**, **2048** (the default value), or **4096**.

- 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.

Routing Protocols

- Starting in Junos OS Release 15.1X49-D80, **authentication-key-chain** configuration is not supported on SRX devices.

System Logs

- Starting with Junos OS Release 15.1X49-D80, two new system log messages have been added to indicate memory-related problems on the interfaces to the DDR3 memory:

  - XMCHIP_CMERROR_DDRIF_INT_REG_CHKSUM_ERR_MINOR
  - XMCHIP_CMERROR_DDRIF_INT_REG_CHKSUM_ERR_MAJOR

  These error messages indicate that the XMCHIP on an Flexible PIC Concentrator (FPC) has detected a checksum error, which is causing packet drops.

  The following error threshold values classify the error as a major error or a minor error:

  - Minor error —> 5 errors per second
  - Major error —> 255 errors per second (maximum count)

- Starting in Junos OS Release 15.1X49-D70, new parameters are added to the structured log fields of the antivirus, antispam, content, and apppxy system log messages.

  The following example shows the structured log fields of **AV_VIRUS_DETECTED_MT, ANTISPAM_SPAM_DETECTED_MT, CONTENT_FILTERING_BLOCKED_MT, APPPXY_RESOURCE_OVERUSED_MT, and APPPXY_SESSION_ABORT_MT** messages before Junos OS Release 15.1X49-D70:

AntiVirus: Virus detected: from <source-address>:<source-port> to <destination-address>:<destination-port> source-zone <source-zone-name> <filename> file <temporary-filename> virus <name> URL:<url> username <username> roles <roles>

AntiSpam: SPAM detected: <source-name> (<source-address>) <action> reason: <reason> username <username> roles <roles>

Content Filtering: <argument> (<profile-name> from <source-address> is <action> due to <reason> username <username> roles <roles>

ApplicationProxy: Suspicious client <source-address>:<source-port>->(<destination-address>:<destination-port>) used <percentage-value> connections, which exceeded the maximum allowed <maximum-value> connectionsusername <username> roles <roles>

ApplicationProxy: session from <source-address>:<source-port> to <destination-address>:<destination-port> aborted due to <error-message> (code <error-code>)

The following example shows **AV_VIRUS_DETECTED_MT, ANTISPAM_SPAM_DETECTED_MT, CONTENT_FILTERING_BLOCKED_MT, APPPXY_RESOURCE_OVERUSED_MT, and APPPXY_SESSION_ABORT_MT** messages in Junos OS Release 15.1X49-D70, indicating the newly added parameters in the structured log fields:

AntiVirus: Virus detected: <source-address>:<source-port>-><destination-address>:<destination-port> source-zone="<source-zone-name>" profile-name="<profile-name>" file="<filename>" temp_file="<temporary-filename>" virus="<name>" URL="<url>" username="<username>" roles="<roles>"

AntiSpam: SPAM detected: name="<source-name>" source-ip=(<source-address>) profile-name="<profile-name>" action="<action>" reason="<reason>" username="<username>" roles="<roles>"

Content Filtering: protocol="<argument>" <source-address>:<source-port>-><destination-address>:<destination-port> profile-name="<profile-name>" action="<action>" reason="<reason>" username="<username>" roles="<roles>"

ApplicationProxy: Suspicious client <source-address>:<source-port>->(<destination-address>:<destination-port>) used <current-connections> connections, which exceeded the maximum allowed <maximum-value> connections. policy-name <policy-name> username <username> roles <roles>

ApplicationProxy: session from <source-address>:<source-port> to <destination-address>:<destination-port> aborted due to <error-message> (code <error-code>), policy-name <policy-name>

VPNs

- Starting with Junos OS Release 15.1X49-D80, the **xauth access-profile** option is being deprecated at the [**edit security ike gateway *gateway-name***] hierarchy level, and will

no longer be supported in a future release. A new configuration option **aaa access-profile** is added under [**edit security ike gateway *gateway-name***] hierarchy level for Extended Authentication (XAuth) and Extensible Authentication Protocol (EAP) authentication. Also, **AAA** replaces the **XAuth** field names in the outputs for the **show security ike active-peer**, **show security ike active-peer detail**, **show security ike security-association detail**, and **show security ipsec next-hop-tunnels** commands.

- The **show security dynamic-vpn client version** command is not supported for dynamic VPN.
- Starting with Junos OS Release 15.1X49-D70, a warning message is displayed if you configure the **establish-tunnels immediately** option at the [**edit security ipsec vpn *vpn-name***] hierarchy level on AutoVPN hubs with point-to-point tunnel interfaces. Committing the configuration will succeed, however the **establish-tunnels immediately** configuration is ignored. The state of the point-to-point tunnel interface will be up all the time.

  The **establish-tunnels immediately** option is not appropriate for AutoVPN hubs with point-to-point tunnel interfaces because multiple VPN tunnels may be associated with a single AutoVPN configuration.

Related Documentation

- New and Changed Features on page 4
- Resolved Issues on page 24
- Known Behavior on page 14
- Known Issues on page 19
- Migration, Upgrade, and Downgrade Instructions on page 30

Known Behavior

This section contains the known behaviors, system maximums, and limitations in hardware and software in Junos OS Release 15.1X49-D80.

AppSecure

- When an SRX Series device is operating in chassis cluster mode (Active/Active mode - Z mode) **show services application-identification statistics applications** and **show services application-identification statistics application-groups** command outputs do not provide complete statistics for bytes count for the session in application/application group statistics. This is because, ingress and egress traffic byte counts are updated separately on the primary and secondary nodes in the chassis cluster setup for a given application.

Class of Service (CoS)

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.
- Only route-based VPN can apply st0 CoS. Table 1 on page 15 describes the st0 CoS feature support for different types of VPN.

Table 1: 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 SRX300, SRX320, SRX340, SRX345, and SRX550M 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 SRX300, SRX320, SRX340, SRX345, and SRX550M 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-system limitation. This is the same policer behavior as on the physical interface.

Ethernet Switching

- On SRX300, SRX320, SRX340, SRX345, and SRX550M devices, when you create an aggregated interface with two or more ports and set the **family** to Ethernet switching, and if a link in the bundle goes down, the traffic forwarded through the same link will be rerouted two seconds later. This causes an outage for the traffic being sent to the link until reroute is complete.
- SRX300, SRX320, SRX340, SRX345, and SRX550M devices do not support Connectivity Fault Management (CFM) packet level filtering. SRX Series devices do not forward the Link Trace Messages (LTMs) packets through Layer 2 engine if any CFM MPs configured on the device. You must configure maintenance association intermediate points (MIPs) on the intermediate device to pass the LTM packets to the other device.
- In Junos OS Release 15.1X49-D40, the Three-color policer feature is not supported on SRX Series devices and vSRX instances.

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.

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 Series 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.

Interfaces and Routing

- On SRX300, SRX320, SRX340, SRX345, and SRX550M, after you upgrade to Junos OS 15.1X49-D50 or later, the automatic medium-dependant interface crossover (auto-MDIX) feature gets disabled when autonegotiation is disabled. To configure the auto-MDIX feature to be always enabled, especially when autonegotiation is disabled, use the **set interfaces *interface name* ether-options mdi-mode force** command.

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 and SRX550M 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, SRX4100, SRX4200, SRX5400, SRX5600, and SRX5800 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.

VPNs

- The default dead peer detection (DPD) settings on the NCP Exclusive Remote Access Client specify sending messages at 20-second intervals for a maximum of eight times. When chassis cluster failover occurs, the SRX Series devices might not recover within the parameters specified by the DPD settings and the tunnel goes down. In this case, increase the DPD interval on the NCP Exclusive Remote Access Client to 60 seconds.
- TCP connections from NCP Exclusive Remote Access Clients use port 443 on SRX Series devices. Device management on TCP connections, such as J-Web, also use port 443 on SRX Series devices. If the J-Web connection uses a port other than 443, tcp-encap must be configured for host-inbound system services. Use the **set security zones security-zone *zone* host-inbound-traffic system-services tcp-encap** command. (IKE must also be configured for host-inbound system services using the **set security zones security-zone *zone* host-inbound-traffic system-services ike** command.)

  To prevent NCP Exclusive Remote Access Client and J-Web connections on port 443, use the **except** option with https and tcp-encap system services. If the J-Web connection uses a port other than 443, use the **set security zones security-zone *zone* host-inbound-traffic system-services tcp-encap except** command to block NCP Exclusive Remote Access Client connections.
- If the IKE external interface is disabled then enabled, tunnels that use TCP connections with NCP Exclusive Remote Access Clients may not come up. If this occurs, reduce the TCP timeout for the client connections with the **inactivity-timeout** option at the [**edit applications application *application-name***] hierarchy level. The **destination-port** configured at the [**edit applications application *application-name***] hierarchy level must

match the **ports** option configured at the [**edit security tcp-encap profile** *profile-name*] hierarchy level. The configuration application must then be specified in the **match application** configuration at the [**edit security policies from-zone** *from-zone* **to-zone** *to-zone* **policy** *policy-name*] hierarchy level.

Tunnels that use TCP connections might not survive ISSU if the dead peer detection (DPD) timeout is not large enough. If you see this happening, increase the DPD timeout to a value greater than 120 seconds. The DPD timeout is a product of the configured DPD interval and threshold. For example, if the DPD interval is 32 and the threshold is 4, the timeout is 128

- ISSU with VPN configuration is not supported when upgrading from a Junos OS release prior to 15.1X49-D75 to Junos OS Release 15.1X49-D75 and later releases. You can use ISSU with VPN configuration when upgrading from Junos OS Release 15.1X49-D75 to later releases. You can also use ISSU with VPN configuration to upgrade from Junos OS Release 15.1X49-D10 up to Junos OS Release 15.1X49-D70.
- On SRX Series devices, configuring RIP demand circuits over P2MP VPN interfaces is not supported.
- On SRX5400, SRX5600, and SRX5800 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 4
- Changes in Behavior and Syntax on page 9
- Known Issues on page 19
- Resolved Issues on page 24
- Migration, Upgrade, and Downgrade Instructions on page 30

Known Issues

This section lists the known issues in hardware and software in Junos OS Release 15.1X49-D80.

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

Authentication and Access Control

- On SRX5600 devices, DNS and WIN IPs are in reverse order in **active-peer** output when configured at access level and access profile level. PR1252186

Chassis Clustering

- On SRX Series devices, the reth interface takes 11 seconds to go down after the reth sub-interface goes down to avoid interface flap. As a workaround, bring the reth interface down immediately when all the reth sub-interfaces are down. PR1064132

CLI

- On SRX1500 devices, traces cannot be enabled or disabled through the CLI options under **tcp-encap traceoptions**. PR1252544

Ethernet Switching

- On SRX300, SRX320, SRX340, SRX345, and SRX550M devices, the current Ethernet switching MAC aging is using software to age out bulk learned MAC addresses. You cannot age out specific MAC address learned at specific time immediately after the configured age. Theoretically, the MAC address might be aged out close to two times the configured age out time. PR1179089
- On SRX Series devices, the **show arp** command will show all the ARP entries learned from all interfaces. When Layer 2 global mode is switching, the ARP entries learned from IRB interface can only show one specific VLAN member port instead of the actual VLAN port learned in the ARP entries. PR1180949
- On SRX1500 devices configured in Ethernet switching mode, only few MAC entries are shown in the output of **show ethernet-switching table** command, even after MAC age out time. This issue is applicable only when MAC learning table has more than 17000 MAC entries. PR1194667
- On SRX300, SRX320, SRX340, and SRX345 devices, you cannot launch setup wizard after using the reset configuration button when the device is in Layer 2 transparent mode. You can launch the setup wizard by using the reset configuration button on the device when the device is in switching mode. PR1206189
- On SRX345 and SRX550M devices, frame carried with priority bit on Tag Protocol Identifier (TPID) will be lost when packet passes through with Layer 2 forwarding. PR1229021
- On SRX300, SRX320, SRX340, SRX345, and SRX550M devices, after certain period of enabling dot1x, multiple first message EAP frames with the same timestamp are transmitted. However, this does not affect any dot1x functionality. PR1245325
- On SRX345 devices, sometimes it is observed that either on primary or the secondary node, the switching fab probe status is down in Layer 2 HA configuration. The Layer 2 HA traffic can work well under such state. This state will move to up on rebooting both nodes. PR1257617

Flow-based and Packet-based Processing

- On SRX5400, SRX5600, and SRX5800 devices, in central point architecture, system logs are sent per second per SPU. Hence, the number of SPUs define the number of system logs per second. PR1126885
- On SRX1500 devices, the log buffer size is increased to 30,000 in event mode. When the log buffer size 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, NP error occurs when service offline is enabled on NP-IOC. PR1210152
- On SRX1500, SRX4100, and SRX4200 devices, the RPM firewall counter increases the best-effort traffic class when **probe-type**, **tcp-ping**, and **dscp-code-points** CS7 are configured. PR1212678
- On SRX300, SRX320, SRX340, and SRX345 devices, when Juniper USB with part number RE-USB-4G-S (740-028898) is inserted in the USB slot while the device is ON, the device reboots. PR1214125
- On SRX Series devices with Selective Packet Services configured, multicast traffic might be sent out-of-order by the device. PR1246877
- On SRX345 devices, when you use the NCP remote access client with the TCP encapsulation (Pathfinder) setting enabled, only one Data Plane Redundancy Group (RG1+) can be used. When you use multiple RG1+ and packets traverse the fabric link (Z-mode traffic), packets will be dropped. PR1263443

Interfaces and Routing

- On SRX1500 devices, when 1G SFP-T is used on the 1G SFP ports (ge-0/0/12 to ge-0/0/15), the ge interface does not operate at 100M speed. PR1133384
- On SRX300, SRX320, SRX340, SRX345, and SRX550M devices, for IFLS (logical interface) scaling:
  - Without **per-unit-scheduler** configured, total IFL number is limited to 2048.
  - With **per-unit-scheduler** configured on the IFD interface: total IFL number is limited to CoS scheduler sub-unit upper limit (2048). So, IFL max-number for **per-unit scheduler** should be 2048 minus the number of physical interface (which is up with at least one logical interface up, max number is 128). PR1138997
- On SRX5600 devices, when CoS on st0 interface is enabled and the incoming traffic rate destined for st0 interface is higher than 300000 packets per second (pps) per SPU, the device might drop some of the high priority packets internally and shaping of outgoing traffic might be impacted. It is recommended that you configure appropriate policer on the ingress interface to limit the traffic below 300000 pps per SPU. PR1239021
- On SRX550M devices, traffic loop is seen with MSTP for untag traffic from IxNetwork ports. Configuring **native-vlan id** on the interfaces connected to IxNetwork port will remove the loop. PR1259099

J-Web

- On SRX Series devices, when you configure a policy on J-Web, the address set is seen as undefined in the Policy wizard. However, if a policy is created from Security > Policy > Apply policy, the address set is seen. PR892766
- On SRX Series devices, all fields in the edit policy window are empty in the logical systems. PR900975
- On SRX Series devices, Korean language description is broken on J-Web. PR943989
- On SRX Series devices, you cannot open the 'Edit Radio' window if there is a wpa-enterprise configured for virtual-access-point. PR945039
- On J-Web, the App-FW page does not show the counter information. PR972473
- On SRX Series devices in chassis cluster, when the switch to Layer 2 mode button is pressed in J-Web, it does not ask for any confirmation and converts to transparent mode immediately and reboots the device. PR1007740
- On SRX Series devices, the PKI certificate issued by J-Web GUI HTTPs will not be used when DVPN is configured in the same device. This is because the device will use the self-signed PKI certificate for both J-Web GUI HTTPs and DVPN URL access. PR1017747
- On SRX Series devices, the J-Web Dashboard does not show correct LED color for alarm status. PR1026883
- On SRX Series devices, when you navigate to the Monitor>NAT>Source NAT page and click the Resource Usage tab, all Pool type values in the grid are displayed as PAT. J-Web fails to recognize the Non-PAT pool. PR1036621
- On SRX5600 and SRX5800 devices, link to rescue on the Dashboard board is not visible for Junos OS Release 15.1X49-D10. PR1096208
- On SRX Series devices, when a user logs in to J-Web using logical system (LSYS) credentials, the user cannot monitor the CPU profile on the Dashboard page. PR1097008
- On SRX550M and SRX1500 devices, there is no option to configure Layer 2 firewall filters from J-Web irrespective of the device mode. PR1138333
- On SRX Series devices in chassis cluster, if you want to use J-Web to configure and commit the configurations, you must ensure that all other user sessions are logged out including any CLI sessions. Otherwise, the configurations might fail. PR1140019
- SRX300, SRX320, SRX340, SRX345, and SRX550M devices do not have dedicated management and control port. The HA wizard for SRX300, SRX320, SRX340, and SRX345 devices use ge-0/0/3 as the management port to access J-Web, post-HA configurations. Working with ge-0/0/3 mandates you to be near the device (possible to access the device in switched private network also) and automatically configures a private IP to the interface ge-0/0/3. It also configured 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 implementation of HA configuration Wizard for SRX300, SRX320, SRX340, SRX345, and SRX550M devices. If a user unknowingly makes the secondary device up, the J-Web would get stuck and further configuration is not allowed.

For example, fab port or some optional configuration could get missed and the complete HA configuration might not happen. PR1142955

- On SRX Series devices in J-Web, when you login to the Web-authentication page, BAD_PAGE_FAULT will be seen. PR1180787
- On SRX1500 devices in J-Web, snapshot functionality Maintain->Snapshot->Target Media->Disk ->Click Snap Shot is not supported. PR1204587
- On SRX Series devices, DHCP relay configuration under Configure > Services > DHCP > DHCP Relay page is removed from J-Web in Junos OS Release 15.1X49-D60. The same DHCP relay can be configured using the CLI. PR1205911
- On SRX Series devices, DHCP client bindings under Monitor is removed for Junos OS Release 15.1X49-D60. The same bindings can be seen in CLI using the **show dhcp client binding** command. PR1205915
- On SRX Series devices, if the load is more than 5000 bytes then the J-Web the responds slowly and the navigation of pages will take more time. PR1222010
- On SRX4100 devices, a security policy page in J-Web does not load when it has 40000 firewall policy configuration. Navigate to Configure> Security> Security Policy page. PR1251714
- On SRX340 and SRX345 devices, on the Setup Wizard default mode, an address pool is created for a management IP network even if you change the default management IP address in the **default-setup** mode. PR1259742

Platform and Infrastructure

- On SRX Series devices, when a USB flash device with a mounted file system is physically detached by a user, the system might panic in such situation. This is a known FreeBSD issue which is resolved in version 7.3 and later. PR695780
- On SRX5800 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 more sessions are required for SOF or lower the SOF session amount to make sure IOC2 is capable of handling it. PR1121262
- On SRX5800 devices, if the system service REST API is added to the configuration, though commit can be completed, all the configuration changes in this commit will not take effect. This occurs as the REST API daemon fails to come up and the interface IP is not available during bootup. The configuration is not read on the Routing Engine side. PR1123304
- On SRX4100 and SRX4200 devices, although the CLI is configurable, the following features are not supported: Group VPN, VPN Suite B, and encrypted control links when in chassis cluster. PR1214410

Unified Threat Management (UTM)

- On SRX Series devices with Sophos Antivirus (SAV) configured, some files that have size larger than the **max-content-size** might not go into fallback state. Instead, some protocols do not predeclare the content size. PR1005086

Upgrade and Downgrade

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

VPNs

- On SRX Series devices, if IPsec VPN tunnel is established using IKEv2, due to bad SPI, packet drop might be observed during CHILD_SA rekey when the device is the responder for this rekey. PR1129903
- On SRX Series devices in chassis cluster, IPsec VPN tunnel which uses a PPPoE interface as the external interface will fail after RG0 failover. PR1143955
- On SRX5800 devices, when upgrading from Junos OS Release 15.1X49-D30 to 15.1X49-D35, 15.1X49-D40, and 15.1X49-D50 and from 15.1X49-D35, 15.1X49-D40, and 15.1X49-D50 to 15.1X49-D60 release, the ISSU fails for AutoVPN/ADVPN/DEP IPsec VPN tunnels. PR1201955
- On SRX5400, SRX5600, and SRX5800 devices, IPSec VPN traffic might be dropped if the IPSec tunnel is in different routing instances, and needs to be routed by routing-instance in a NAT rule. PR1217583
- On SRX1500 devices, if DPD is configured for **tcp-encap** sessions, then the effective DPD timeout must be increased to greater than 120 seconds. PR1254875

Related Documentation

- New and Changed Features on page 4
- Migration, Upgrade, and Downgrade Instructions on page 30
- Changes in Behavior and Syntax on page 9
- Known Behavior on page 14
- Resolved Issues on page 24

Resolved Issues

This section lists the issues fixed in hardware and software in Junos OS Release 15.1X49-D80.

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 SRX Series devices, MGCP ALG complex calls (group or ACD calls) are not working as expected. PR1226822
- On SRX Series devices, Trivial File Transfer Protocol (TFTP) ALG logging does not recognize the service TFTP when both the source port and destination port are not known ports. PR1232026

Chassis Clustering

- On SRX1500, SRX4100, and SRX4200 devices, the front panel alarm LED does not turn amber even when the device has minor system alarm. PR1227138
- On SRX320 and SRX320-POE devices in chassis cluster, when configuring Ethernet switching, the device reboots followed by a CLI warning message. Rebooting only one node in the chassis cluster setup might lead to asynchronized chassis cluster status that is not supported, and this might result in the device moving to database mode. Reboot both the nodes in chassis cluster setup together to avoid the issue. PR1228473
- On SRX300 devices in chassis cluster, PPPoE fails to establish session when RG0 and RG1 primary node is asymmetric. PR1230627
- On all SRX Series devices in chassis cluster, the configuration synchronization monitoring might fail if the following configuration is enabled: **set system encrypt-configuration-files**. The configuration synchronization monitoring failure might result in disabling the secondary node after reboot. PR1235628
- On SRX345 devices in chassis cluster, secondary node fails to update AppID signature using the scheduled update. PR1237421
- On SRX devices in chassis cluster, ICMP redirect is not sent from a reth interface for a route advertised by BGP. PR1249322
- On SRX1500 devices, IP leak might occur under the following circumstances in a HA environment:
  - In case of IKEv1, it is possible for an IPsec VPN tunnel to be active without an active IKEv1 phase 1 SA. Since the assigned IP address associated with an IPsec VPN tunnel (for a user) is stored in the record of phase 1 SA, if HA RG0 failover occurs while there is no active IKEv1 phase SA exist for an IPsec VPN tunnel, the assigned IP address will be released to the authd daemon when the IPsec VPN tunnel is disconnected.
  - In case a remote access IPsec VPN tunnel is cleared (for both IKEv1 and IKEv2), the assigned IP address is kept for 30 seconds before it is released back to the authd within an additional 2 minutes. If HA failover occurs during this time before the IP is received at the authd, there will be an IP address leak.
  - If a new IP is assigned by authd daemon after every user is authenticated, regardless of the user already having an IP assigned from an early authentication. In case of IKEv1, authentication occurs at every IKE phase 1 SA rekey. If the KMD daemon restarts immediately (within 2 minutes) after an IKEv1 phase 1 SA rekey, there is a possibility

that the newly assigned IP has not been released to authd daemon yet. This will lead to the leak of that IP.

PR1252181

CLI

- On SRX1500 devices, the CLI commands **request pppoe connect** and **request pppoe disconnect** do not work. PR1231804

Ethernet Switching

- On SRX1500 devices in Ethernet switching mode, an IRB interface located in a custom routing-instance is not reachable. PR1234000
- On SRX Series devices, ndrapol and delegated-pool cannot use the second range. PR1234243
- On SRX Series devices, use prefix-length mask-low or mask-high to configure ndrapool and delegated pool, and to open jdhcpd trace and coredump PR1236167
- On SRX300, SRX320, SRX340, and SRX345 devices, the value of managed (M) bit cannot be reset if it is configured as true. PR1236548
- The flowd process might generate a coredump when running trace options for the cascaded DHCP with IPv6 prefix delegation. PR1242036
- On SRX300, SRX320, SRX340, SRX345, and SRX550M devices, when you attempt to commit **vlan-id** with range 4094, commit fails with error **error: Value 4000 is not within range (1..3967)**. PR1246316

Flow-based and Packet-based Processing

- On XL-based cards such as MPC or IOC3, PPE thread timeout errors are triggered when the FPC allocates illegal memory space for forwarding state of routing operations. In certain cases, this results in packet loss depending on the number of packets using this forwarding state. PR1100357
- If a device receives ICMP request or reply with same source IP, destination IP and, sequence number of existing ICMP session that has already received a response, instead of being marked for closure this results in session timeout refreshed. PR1202432
- In a chassis cluster, some traffic destined to or sourced from the SRX itself might be dropped when applying application framework services to this traffic while the control plane and data plane are active on different nodes. PR1210018
- On SRX Series devices, the flowd process might crash after committing a configuration regarding the MTU on an interface with PIM tunnel enabled, such as, after committing MTU set to 9192 (maximum allowed by configuration) on the main interface and set the IP MTU to 1500 on all sub interfaces while the PIM is operational. PR1224808
- On SRX Series devices, when services-offload is used for multicast handling and fragmented multicast packets are processed the flowd process might crash, generating

a coredump. This results in the data plane of the processing device being restarted. PR1233849

- On SRX Series devices, the flowd process might crash when NAT46 session activeness changes from Z-mode operation to active-backup mode at the same time fragment packet belong to that session is being processed. PR1233879
- On SRX5800 devices, the output of counters for individual mirror-filters for X2-Mirroring displays 0. PR1234449
- On SRX5800 devices, flowd coredump occurs when using X2 traffic monitoring feature between IPsec tunnels. PR1236253
- On SRX5400, SRX5600, and SRX5800 devices, when using Internet Key Exchange (IKE) in chassis cluster, memory buffer (mbuf) stall might trigger FPC alarms and RG failover. PR1236672
- On SRX4200 devices in chassis cluster, the flowd process might crash and generate coredump under the following conditions: IPv6 IPsec VPN tunnel is established NAT is enabled for the IPv6 VPN traffic Performing failover for the VPN traffic related data-plane Redundancy Group (RG). PR1237311
- On SRX5400, SRX5600, and SRX5800 devices, Bidirectional Forwarding Detection (BFD) multihop for IPv6 does not work. PR1239016
- On SRX345 devices, firewall operating in transparent mode, any link down interface on the VLAN might cause multicast traffic drop. PR1246084
- On SRX5600 devices, the flowd process might crash and generate coredump when SecIntel (security-intelligence) is configured. PR1246679

Interfaces and Routing

- On SRX300, SRX320, SRX320-POE, SRX340, SRX345, and SRX 550M devices the IRB interface cannot be used as an external interface with the IPsec VPN. PR1166714
- On SRX Series devices, when an ARP entry is learned through an AE interface and a route is pointing to that ARP next hop, the ARP entry will not expire even if the ARP IP is not reachable. This issue occurs due to the route nexthop on the AE interface getting stuck in a unicast state even if the remote end is not reachable, and the RPD is unaware that the ARP is invalid. So, with this resolution, the route nexthop on the AE interface can be shown in the hold state when the remote end is not reachable. PR1211757
- On Q-in-Q port of the SRX340, SRX345, and SRX550M devices, the IRB interface works on the native VLAN ID. PR1225926
- On SRX550M devices, when the monitor traffic interface command is run for first time after reboot, and then stopped, forwarding in VPLS and Layer 2 circuits might stop. Forwarding is active again when the monitor traffic interface command is enabled, and stops when the monitor traffic interface command is disabled. PR1233209
- On SRX5600 devices, if st0 interface is moved from one routing instance to another routing instance, there might be some traffic disruption. PR1241505

J-Web

- On SRX Series devices, on the J-Web dashboard page, the refresh button does not work properly. This does not provide correct color of the HA LED nor the Interface LED. PR1232076
- On SRX devices, J-Web does not display all application tracking results. PR1239705
- On SRX340 devices, in a J-Web configuration, commit would fail when disabling the functions at "Authentication Source Priority Configuration". PR1241675

Network Address Translation (NAT)

- On SRX Series devices, high memory utilization might be observed on the RE due to a memory leak in the NSD process, caused by the SNMP polling of NAT statistics. PR1226337

Platform and Infrastructure

- On SRX5400, SRX5600, and SRX5800 devices, the flowd process might crash when services offload (SOF) is enabled. PR1084123
- When using the **request system software** command along with the **partition** and **validate** options, the current configuration is not validated against the Junos version being upgraded to as part of the upgrade process. PR1223443
- On SRX5400, SRX5600, and SRX5800 devices, the log message **Warning! random engine is holding busy** is displayed frequently in **/var/log/messages**. PR1233408
- On SRX Series devices, due to a regression issue, presence of errors or traps during ISSU might result in LU/XL based FPC crash. PR1239304
- SRX1500 devices might shutdown due to an incorrect reading from the temperature sensor. Log messages similar to the following messages might appear in the lcmd log:

  :srx_shutdown:214: called with FRU TmpSensor
  :ALARM [SET -> Time: Nov 10 09:00:31, Name: FE Board Phy0 , Short Reason: TSensor X Too Hot , Long Reason: TSensor X:FE Board Phy0 Too Hot]

  PR1241061
- On SRX4100, and SRX4200 devices J-Flow v9 sampling is configured. After packets are sampled on the device, capture these flow record packets. The value of **SrcMask**, **DstMask**, **srcas**, **dstas**, **snmp_index** for incoming or outgoing interface is incorrect within the captured frames. IPv4 flow and IPv6 flow have the same issue. PR1241965
- On SRX5400, SRX5600, and SRX5800 devices running Junos OS Release 15.1X49-D30 and later, enabling datapath-debug may trigger flowd coredump on multiple SPCs if the device was forwarding traffic that requires flow serialization (for example, IDP, JDPI, and ALG). PR1248657

Routing Policy and Firewall Filters

- On all SRX Series devices, when there is at least one policy using the range address in a zone, the network security daemon (NSD) crashes after executing show security shadow-policies command. PR1232736

Routing Protocols

- On all SRX devices, when OSPF dead-interval is lower than the default value, graceful restart might not work during manual RG0 failover or ISSU, causing service disruption. PR1216687

Simple Network Management Protocol (SNMP)

- On SRX340 devices, SNMP MIB OIDs jnxOperating1MinAvgCPU (Routing Engine CPU usage) always returns 100. PR1237331
- On SRX1500 devices, SNMP traps are not generated when power cable is plugged out or when one of the PSU is plugged-in or plugged out from the device. PR1242827

System Alarms

- On SRX1500 devices starting with Junos OS Release 15.1x49-D75, **FPC 0 PEM 1 Removed** alarm is seen even though PEM1 is not inserted. PR1232364

VPNs

- On SRX5600 devices, when tunnels are cleared between the client and the SRX5600 cluster, and RG0 failover on the SRX5600 devices, there might be instances where tunnels do not come up initially. PR1227433
- On SRX300, SRX320, SRX320-POE, SRX340, and SRX345 devices, when you configure IPsec authentication with manual security associations, the device might crash. PR1230491

Related Documentation

- New and Changed Features on page 4
- Migration, Upgrade, and Downgrade Instructions on page 30
- Changes in Behavior and Syntax on page 9
- Known Behavior on page 14
- Known Issues on page 19

Documentation Updates

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

- Starting in Junos OS Release 15.1X49-D80, information from *Chassis Cluster Feature Guide for Branch SRX Series* and *High-End SRX Series Devices* is combined as a new

Chassis Cluster Feature Guide for Security Devices. This guide caters to chassis cluster information for all SRX Series devices. See Chassis Cluster Feature Guide for Security Devices.

- Information about MIBs is available in SNMP MIBS Explorer. On the Junos OS for SRX Series 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.
- Information about system log messages is available in System Log Explorer. On the Junos OS for SRX Series 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

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 http://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 32).

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.

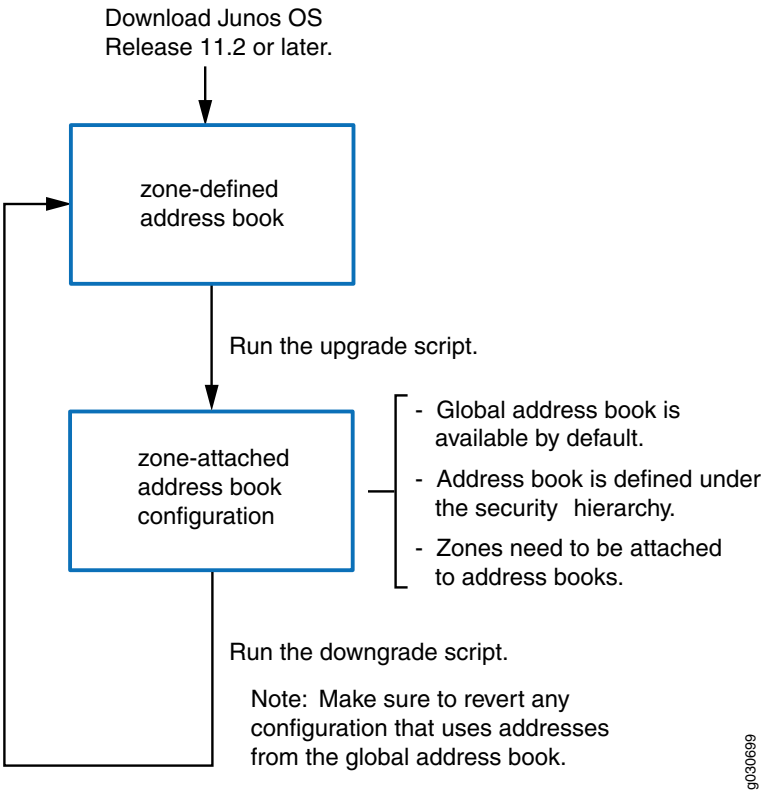
  After upgrading to the zone-attached address book configuration:

  - 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 Release 12.3X48 is an EEOL release. You can upgrade from Junos OS Release 12.1X46 to Release 12.3X48 or even from Junos OS Release 12.3X48 to Release 15.1X49-D10. For upgrading from Junos OS Release 12.1X47-D15 to Junos OS Release 15.1X49-D10, ISSU is supported. However, you cannot upgrade directly from a non-EEOL release that is more than three releases ahead or behind.

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

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

For information about software installation and upgrade, see the Installation and Upgrade Guide for Security Devices.

For information about ISSU, see the Chassis Cluster Feature Guide for Security Devices.

Related Documentation

- New and Changed Features on page 4
- Changes in Behavior and Syntax on page 9
- Known Behavior on page 14
- Known Issues on page 19
- Resolved Issues on page 24

Product Compatibility

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

- Hardware Compatibility on page 33
- Transceiver Compatibility for SRX Series Devices on page 34

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 http://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 http://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.

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 http://pathfinder.juniper.net/feature-explorer/.

Juniper Networks Content Explorer is a Web-based application that helps you explore Juniper Networks technical documentation by product, task, and software release, and download documentation in PDF format. Find Content Explorer at http://www.juniper.net/techpubs/content-applications/content-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 http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit http://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: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: http://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://tools.juniper.net/SerialNumberEntitlementSearch/

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 http://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, see http://www.juniper.net/support/requesting-support.html.

Revision History

30, May 2017—Revision 4— Junos OS 15.1X49-D80 – SRX Series.

12, April 2017—Revision 3— Junos OS 15.1X49-D80 – SRX Series.

3, April 2017—Revision 2— Junos OS 15.1X49-D80 – SRX Series.

23, March 2017—Revision 1— Junos OS 15.1X49-D80 – SRX Series.