Release Notes: Junos® OS Release 15.1X49-D70 for the SRX Series

Release 15.1X49-D70
2 January 2018
Revision 10

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-D70 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-D70 supports the following devices:

- Branch SRX Series devices: SRX300, SRX320, SRX340, SRX345, and SRX550 High Memory (SRX550M)
- Mid-range SRX Series devices: SRX1500, SRX4100, and SRX4200. These mid-range devices are referred as SRX1500, SRX4100, and SRX4200 in this Release Notes.
- High-end SRX Series devices: 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).
- vSRX

For more details about SRX Series high-end 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-D70 for the SRX Series devices.

- Release 15.1X49-D70 Software Features on page 5

Release 15.1X49-D70 Software Features

Chassis Cluster

- **ISSU support on SRX1500 devices**—Beginning with Junos OS Release 15.1X49-D70, SRX1500 devices support In-service software upgrade (ISSU).

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

  An 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.]

- **Second Routing Engine startup details for SRX5600 and SRX5800 devices**—Starting in Junos OS Release 15.1X49-D70, you can view the serial number and hardware version details of the second Routing Engine by using the **show chassis hardware** command. On SRX5000 line of devices, you require a second Routing Engine for configuring dual control links in chassis cluster mode.

  The second Routing Engine performs a normal startup and is used only for the backup control link.

  NOTE: **Dual control is not supported on the SRX5400 Series Devices because of limited slots on the device.**

  [See Upgrading the Second Routing Engine When Using Chassis Cluster Dual Control Links on SRX5600 and SRX5800 Devices and show chassis hardware (View).]

Class of Service

- **CoS support for the st0 interface for SRX Series devices and vSRX instances**—Starting with Junos OS 15.1X49-D70, 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. The following CoS features are supported on all available SRX Series devices and vSRX2.0:

- Classifiers
- Policers
- Queuing, scheduling, and shaping
- Rewrite markers
- Virtual channels

See Class of Service Feature Guide for Security Devices.

Dynamic Host Configuration Protocol (DHCP)

- **Cascaded DHCPv6 Prefix Delegation on SRX Series Devices**—The cascaded DHCPv6 prefix delegation feature is supported in Junos OS Release 12.3X48-D40 and in Junos OS Release 15.1X49-D70 and later. This feature allows the customer premises equipment (CPE) to delegate sub-prefixes to sub-CPEs and assign IPV6 addresses to end hosts through stateless address autoconfiguration (SLAAC), stateless DHCPv6, or stateful DHCPv6. The LAN interface supports these three kinds of address assignment through independent configurations for DHCPv6, stateless SLAAC, and stateful DHCPv6.

  NOTE: **Only SRX300,SRX320, SRX340, SRX345, and SRX550M support cascaded prefix delegation.**

  [See Understanding Cascaded DHCPv6 Prefix Delegating.]

Ethernet Switching

- **Layer 2 features support for SRX1500 devices**—Starting in Junos OS Release 15.1X49-D70, Layer 2 supports the following features in switching mode:
  - Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), and Multiple Spanning Tree Protocol (MSTP)
  - Classification, policing, queuing, scheduling, and shaping on the integrated routing and bridging (IRB) interface
  - Link fault management (LFM)
- **Layer 2 features support for SRX300, SRX320, SRX340, SRX345, and SRX550M devices**—Starting in Junos OS Release 15.1X49-D70, Layer 2 supports the following features in switching mode:
  - Layer 2 switching capability to the devices in a chassis clusters. This feature allows the use of Ethernet switching features on both nodes of a chassis cluster.
  - Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), and Multiple Spanning Tree Protocol (MSTP).
  - Connectivity fault management (CFM) and link fault management (LFM).

- Q-in-Q VLAN tagging.

  NOTE: Q-in-Q VLAN tagging is supported only on SRX340, SRX345, and SRX550M devices.

- VLAN retagging.
- Multiple VLAN Registration Protocol (MVRP).
- Source address filtering in Layer 2 switching.
- The **allowed-mac** and **shutdown-action** switching options.

Firewall User Authentication

- **User firewall captive portal HTTPS redirect support on SRX300, SRX320, SRX340, SRX345, SRX550M, SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, and SRX5800 devices and vSRX instances**—Starting with Junos OS Release 15.1X49-D70, user firewall captive portal HTTPS redirect provides the following two additional user firewall authentication sources:
  - **web-redirect**: The Packet Forwarding Engine redirects the HTTP/HTTPS request to HTTP WebAuth for user firewall authentication.
  - **web-redirect-to-https**: The Packet Forwarding Engine redirects the HTTP/HTTPS request to HTTPS WebAuth for user firewall authentication.

Flow-based and Packet-based Processing

- **TCP window scale option support on SRX Series devices**—Starting with Junos OS Release 15.1X49-D70, the TCP Window Scale (WS) option on TCP proxy is supported. The TCP WS option is used to enlarge the window scale. The maximum scaled TCP receive window is 1MB and default maximum scaled TCP receive window is 256KB.

  [See Understanding TCP Proxy.]

General Packet Radio Service (GPRS)

- **GTP and SCTP support**—Starting with Junos OS Release 15.1X49-D70, SRX4100, SRX4200 and vSRX devices support the GPRS Tunnelling Protocol (GTP) and the Stream Control Transmission Protocol (SCTP) Application Layer Gateways (ALGs).

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

- **Flow Session Connection Filter Option**—Starting in Junos OS Release 15.1X49-D70, a new flow session filter option (**conn-tag**) is available. You can include this option in a filter to uniquely identify GTP-U and SCTP flow sessions whose traffic you want to trace and monitor for debugging purposes.

  [See Understanding the Flow Session Connection Filter Option. .]

Interfaces and Routing

- **IPv6 GRE tunnel support for SRX Series devices and vSRX instances**—Starting with Junos OS Release 15.1X49-D70, IPv6 generic routing encapsulation (GRE) tunnel is supported on SRX Series devices and vSRX instances. GRE allows the encapsulation of one routing protocol inside another routing protocol.

  NOTE: Earlier releases supported IPv4 GRE tunnels.

  To configure an IPv6 GRE tunnel, you configure the source and destination addresses of the GRE tunnel using IPv6 addresses. Then, create a routing entry that uses the GRE tunnel as egress.

Network Time Protocol

- **NTP time adjustment threshold for SRX300, SRX320, SRX340, SRX345, SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, and SRX5800 devices and vSRX instances**—Starting with Junos OS Release 15.1X49-D70, this feature allows you to configure a NTP adjustment threshold for the NTP service to ensure that an incorrect NTP server can not adjust the time way out of synchronize, which ensure resiliency.

  For example, when there is a larger time difference in configured threshold between the NTP server and the current system, the system rejects or log this time difference for security purposes and also provides the capability to manually synchronize the time with the NTP service.

On-box Logging

- **On-box logging**— Starting with Junos OS Release 15.1X49-D70, SRX1500, SRX4100, and SRX4200 devices, and vSRX instances support all the current SRX Series logging functionality. This release also introduces some modifications to the current logging functionality. The major functionalities introduced are:
  - On-box traffic logging to solid-state drives (SSDs) supports eight external log servers or files.
  - An all-in-one XML file is added that contains all the traffic logs information. The XML file also generates all the logging header files and traffic-log-related documents.

[See Understanding On-Box Logging Functionality.]

Platform and Infrastructure

- **High-priority queue on SPC for SRX5400, SRX5600, and SRX5800 devices with IOC2 and IOC3 line cards**—For the SRX5K-MPC (IOC2), the SRX5K-MPC3-100G10G (IOC3), and the SRX5K-MPC3-40G10G (IOC3), a new configuration option is supported in Junos OS Release 12.3X48-D40 and in Junos OS Release 15.1X49-D70 and later that enables packets with specific DiffServ code point (DSCP) precedence, inet-precedence, IEEE 802.1Q, and DHCPv6 for IPv6 traffic bits to enter a high-priority queue on the SPC on high-end SRX Series devices.

  Junos Release 15.1X49-D70 supports four priorities: high, medium-high, medium-low, and low. Higher-priority queues take precedence over lower-priority queues for forwarding packets to achieve higher rate and lower latency, while ensuring that low-priority queues are not starved (locked out).

  To designate packets for the high-priority or low-priority queues, use the **spu-priority** configuration statement at the **[edit class-of-service forwarding-classes class]** hierarchy level. A value of high places packets into the high-priority queue, and a value of low places packets into the low-priority queue.

Security-Authentication

- **Secure File Transfer Protocol (SFTP) support on Smart Download for SRX Series devices and vSRX instances**— Starting with Junos OS Release 15.1X49-D70, Smart Download SFTP support is independent of the underlying FTP and provides a secured file transfer tunnel.

User Authentication

- **Controlling access to network resources based on the identity of the device used, not the user's identity for SRX Series devices**—Starting with Junos OS Release 15.1X49-D70, you can use the device identity feature for network access control based on the device's identity. There are various reason you might want to use this feature: you might not know the identity of a user, you might not want to use a captive portal to authenticate users, you might not have a network access control system, or you might have switches that do not support 802.1. This feature allows you to configure a device profile that defines attributes of a device that match a number of devices. You specify the device profile name in a security policy to determine how traffic from matching devices is handled.

- **LDAP over TLS/SSL for encryption and peer-authentication for SRX Series devices**—Beginning with Junos OS Release 15.1X49-D70, SRX Series devices support the Transport Layer Security StartTLS extension for LDAP for the firewall user authentication and the integrated user firewall authentication for obtaining username and role information through firewall authentication.

  StartTLS uses the LDAPv3 TLS extension for a secure connection. StartTLS allows protocol data transfers between the LDAP server and client over the TLS layer after successful negotiation between peers. StartTLS upgrades an existing insecure LDAP connection to a secure TLS/SSL connection.

[See Enabling LDAP Authentication with TLS/SSL for Secure Connections.]

VPNs

- **Verification of the IPsec data path before a point-to-point secure tunnel (st0) interface is activated for SRX300, SRX320, SRX340, SRX345, SRX550M, SRX1500, SRX5400, SRX5600, and SRX5800 devices and vSRX instances**—Starting with Junos OS Release 15.1X49-D70, the IPsec data path between VPN tunnel endpoints can be verified before the secure tunnel (**st0**) interface is activated and routes associated with the interface are installed in the Junos OS forwarding table. This feature applies to route-based site-to-site and dynamic endpoint VPNs with **st0** interfaces in point-to-point mode. To configure the IPsec data path verification, use the **verify-path** statement at the [**edit security ipsec vpn *vpn-name* vpn-monitor**] hierarchy level. If the peer tunnel endpoint is behind a NAT device, the **verify-path destination-ip** option must be specified with the original, untranslated IP address of the remote IKE gateway.

  [See Understanding IPsec Data Path Verification.]

- **Group VPNv2 servers and members supported on SRX1500 devices**—Starting with Junos OS Release 15.1X49-D70, SRX1500 devices can operate as Group VPNv2 servers or members that are compliant with RFC 6407, *The Group Domain of Interpretation (GDOI)*. You can configure SRX1500 devices as Group VPNv2 server clusters; server clusters provide group controller/key server (GC/KS) redundancy and scaling for Group VPNv2 members.

  [See Group VPNv2 Overview.]

- **Suite B and PRIME cryptographic suites supported on SRX1500 devices**—Starting in Junos OS Release 15.1X49-D70, Suite B and PRIME cryptographic suites are supported on SRX1500 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 AES-GCM rather than AES-CBC for IKEv2 negotiations.

  [See Understanding Suite B and PRIME Cryptographic Suites.]

Related Documentation

- Changes in Behavior and Syntax on page 10
- Known Behavior on page 26
- Known Issues on page 32
- Resolved Issues on page 37
- Migration, Upgrade, and Downgrade Instructions on page 44

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-D70.

AppSecure

- 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)

- 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

- Starting with Junos OS Release 15.1X49-D65, on SRX4100 and SRX4200 devices, a dedicated fabric port is available for configuring fabric links to forward traffic between the two devices in the cluster. You can also use the dedicated fabric port for configuring dual fabric links on the devices. No configuration is required while using the dedicated fabric port for a single fabric link configuration.
- **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.
- Starting with Junos OS Release 15.1x49-D70, there is a change in the method for calculating the memory utilization by a Routing Engine. The inactive memory is now considered free and is no longer included in the calculation of memory utilization. That is, the value for used memory shown in the output of the **show chassis routing-engine** command decreases and results in more memory to be available for other processes.

CLI

- Starting in Junos OS Release 15.1X49-D70, the **set chassis routing-engine bios uninterrupt** command is introduced on SRX300, SRX320, SRX340, and SRX345 devices to disable user inputs at U-boot and boot loader stage.
- **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**

Ethernet Switching

- **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 (MFD) are supported on Layer 3 interfaces for SRX300, SRX320, SRX340, 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 http://www.juniper.net/support/downloads/?p=srx5400#sw .

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

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

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
```

General Packet Radio Service (GPRS)

- Starting with Junos OS Release 15.1X49-D70, the Serving GPRS Support Node (SGSN) and a Gateway GPRS Support Node (GGSN) of the GTPv1 or GTPv2 nodes cannot communicate with the GTPv0 node. If a device sends a GTPv1 or GTPv2 message to update the tunnels created by GTPv0, these messages are dropped and the GTPv0 tunnel will not be updated.

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

- Starting in Junos OS Release 15.1X49-D70, the grant rate interval of the [**edit interfaces** ***interface-name*** **unit** ***logical-unit-number*** **radio-router credit interval**] statement can be configured in 100 millisecond intervals. Earlier, this interval was configured in seconds.

- 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.

  NOTE: GRE keepalive feature is supported for IPv4.

- **Routing Policy and Firewall Filters**—Starting with Junos OS Release 15.1X49-D70, the **bfd-liveness-detection** command includes the description field. The description is an attribute under the **bfd-liveness-detection** object. This field is applicable only for the static routes.
- IPv4 over IPv6 IP-IP tunnel configuration is not supported on the following platforms:
  - SRX300
  - SRX320
  - SRX340
  - SRX345
  - SRX550M

  If you create an IPv4 over IPv6 IP-IP tunnel configuration, an error message is displayed and commit fails.

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 options are introduced under the **icmpv6** protocol hierarchy:

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

  The **type** option allows you to specify the type of the message. The value of **type** determines the format of the remaining data.

  [**edit security idp custom-attack attack-name attack-type signature protocol icmpv6 code**]

  The **code** option value is dependent on the message **type** value. This option is used to create an additional level of message granularity.

  [**edit security idp custom-attack attack-name attack-type signature protocol icmpv6 identification**]

  The **identification** option allows you to specify a unique value used by the destination system to associate requests and replies.

  [**edit security idp custom-attack attack-name attack-type signature protocol icmpv6 sequence-number**]

  The **sequence-number** option allows you to specify the sequence number of the packet. This number identifies the location of the request/reply in relation to the entire sequence.

  [**edit security idp custom-attack attack-name attack-type signature protocol icmpv6 data-length**]

  The **data-length** option allows you to specify the number of bytes in the data payload.

- 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-D70, the REST API is supported on SRX1500 devices and vSRX instances in addition to 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

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.

Platform and Infrastructure

- 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).

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-D65 and earlier, if a session was closed by an application like Spotlight Secure, the **reason** attribute displayed a message **session closed sm err** under RT_FLOW_SESSION_CLOSE system log message.

  Starting with Junos OS Release 15.1X49-D70, the message in **reason** attribute is changed to **session closed application discard junos-secintel** under RT_FLOW_SESSION_CLOSE system log message.

  The following example shows RT_FLOW_SESSION_CLOSE messages before Junos OS Release 15.1X49-D70:

  Oct 17 16:11:22 kabuto RT_FLOW: RT_FLOW_SESSION_CLOSE: session closed sm err: 4.0.0.1/668->5.0.0.1/37692 0x0 icmp 4.0.0.1/668->5.0.0.1/37692 0x0 N/A N/A N/A N/A 1 1 untrust trust 20019013 0(0) 0(0) 1 UNKNOWN UNKNOWN N/A(N/A) xe-2/2/9.0 UNKNOWN

  The following example shows RT_FLOW_SESSION_CLOSE messages in Junos OS Release 15.1X49-D70, indicating the message change in **reason** attribute:

  Oct 22 11:26:51 kabuto RT_FLOW: RT_FLOW_SESSION_CLOSE: session closed application discard junos-secintel: 4.0.0.3/55770->5.0.0.1/80 0x0 junos-http 4.0.0.3/55770->5.0.0.1/80 0x0 N/A N/A N/A N/A 6 1 untrust trust 30000021 0(0) 0(0) 1 UNKNOWN UNKNOWN N/A(N/A) xe-2/2/9.0 UNKNOWN

- Starting in Junos OS Release 15.1X49-D70, the **no-tls-certificate-check** parameter is visible and disabled by default. When you enable the **no-tls-certificate-check** parameter, the Lightweight Directory Access Protocol (LDAP) server certificate will not be validated.

- 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

- 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>

- Starting in Junos OS Release 15.1X49-D70, on SRX1500, SRX4100, and SRX4200 Series devices and vSRX instances, the **set security log stream ${*stream_name*}** command is required to configure the stream log. The source address and source interface attributes are no longer required.

  On SRX300, SRX320, SRX340, and SRX345 Series devices, the **set security log stream ${*stream_name*} host ${host_IP}** command is required to configure the stream log file with the source address and source interface attributes configuration.

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.
- 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.

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 26
- Known Issues on page 32
- Resolved Issues on page 37
- Migration, Upgrade, and Downgrade Instructions on page 44

Known Behavior

This section contains the known behaviors, system maximums, and limitations in hardware and software in Junos OS Release 15.1X49-D70.

AppSecure

- 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.

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.
- Only route-based VPN can apply st0 CoS. Table 1 on page 27 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 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.

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

- On SRX4000 Series devices, although the CLI is configurable, the following features are not supported:
  - Encrypted control links when in cluster mode
  - Group VPN and VPN Suite B
  - JFlowv9 in chassis cluster configuration.
  - LACP with L2 Transparent Mode

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.
- 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
- 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.

J-Web

- On all 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.
- Branch devices do not have dedicated management and control port. Chassi cluster wizard for SRX300 Series devices use ge-0/0/3 as management port to access J-Web post chassis cluster 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 configured SRX box as a DHCP Server which assigns an IP to the connected device from the same subnet to which this interface belongs.

There is a very thin line on this implementations of chassis cluster configuration wizard for SRX300 Series and SRX550M. While testing it was found that if user unknowingly make the secondary device up the J-Web would stuck at that point and further configuration such as fabricate port or some optional configuration would get missed out and the complete chassis cluster configuration would not happen.

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
- On SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX650 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.

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.

Screens

- On all SRX Series devices:
  - The maximum scaled TCP proxy receive window size is 1 MB, and the default value is 256 KB.

- The scaled TCP proxy session holds more jbufs and mbufs. This impacts the TCP proxy session that was created earlier and the newly created TCP proxy session packet forwarding.
- The scaled TCP proxy session enlarges host transmit speed. This results in the increased SPU and CPU usage.

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.

Unified Threat Management (UTM)

- 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.

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 10
- Known Issues on page 32
- Resolved Issues on page 37
- Migration, Upgrade, and Downgrade Instructions on page 44

Known Issues

This section lists the known issues in hardware and software in Junos OS Release 15.1X49-D70.

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 chassis cluster, after reboot, if the secondary node (RG1) completes cold synchronize (CS) first, this might result in bidirectional RTO synchronization or incorrect direction for RTO synchronization. PR1138502
- On branch SRX Series devices in chassis cluster, when configuring Ethernet switching, the device reboots followed by a CLI warning message. Rebooting only one node in chassis cluster setup might lead to asynchronized chassis cluster status that is not supported, and this might result in the device to go to db mode. Reboot both the nodes in chassis cluster setup together to avoid the issue. PR1228473

Class of Service

- On high-end SRX Series devices, when CoS on st0 interface is enabled and the incoming traffic rate destined for st0 interface is higher than 300K 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 to configure appropriate policer on the ingress interface to limit the traffic below 300K pps per SPU. PR1239021

CLI

- On branch SRX Series devices, the statistics and counters of Security Intelligence and Sky Advanced Threat Prevention (ATP) might not be shown on CLI if frequent chassis cluster failovers are seen along with medium-high traffic going through for a long period of time. PR1234169

Dynamic Host Configuration Protocol (DHCP)

- On SRX300 Series devices, the value of managed (M) bit cannot be reset if it is configured as true. PR1236548

Flow-based and Packet-based Processing

- On SRX5600 and SRX5800 devices with SRX5K-SPC-4-15-320 card installed, after being in operation for 49 days, a CPU timer rollover on card will occur. When CPU rollover occurs, CPU scheduling of keepalives from SRX5K-SPC-4-15-320 to Routing Engine (RE) might fail. This will result in RE triggering reset of all FPCs on local node through chassisd due to loss of keepalives. PR980650
- 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 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 maximum serialization sessions should be increased to 64000. PR1061524
- On branch SRX Series devices, the maximum-sessions value is displayed incorrectly. PR1094721
- On high-end SRX Series 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 branch SRX Series devices, traffic does not pass with the maximum number of logical interfaces eight queues. PR1138997

- On SRX1500 devices, block-drop action option in Command and Control Spotlight Secure policy for custom_url_data feed does not work. PR1141745
- On SRX1500 devices, when CPU usage is very high (above 95%), there is possibility that the connection between AAMW process and PKID process can break. In this case, the AAMW daemon remains in initializing state until that connection is established. PR1142380
- On SRX1500 devices, after you change the revocation configuration of a CA profile, the change cannot be populated to the SSL-I revocation check. It is recommended to change SSL-I configuration to enable or disable certificate revocation list (CRL) checking instead of CA-profile configuration. PR1143462
- On SRX1500 devices in a chassis cluster with 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, then Packet Forwarding Engine (PFE) might stop working. PR1144836
- On SRX Series devices, when Sky Advanced Threat Protection (ATP) inline blocking and IDP are configured together in the same security policy, Sky ATP inline blocking is not supported, but files are still submitted to the cloud for scanning. In this scenario, IDP functionality is not affected. PR1144843
- 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

Interfaces

- 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, and SRX345 devices, when you change the interface mode from **10m/no-auto-10m/no-auto** to **100m/no-auto-100m/no-auto**, interfaces might be down. PR1165942

J-Web

- 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** 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 does not send the second request, because the process detects that the first authentication did not occur. This delay causes memory leak on the authd process and the memory might be exhausted, generating a core file and preventing DHCP server service. High CPU usage on the Routing Engine might also be observed. PR1042818
- On branch SRX Series devices in chassis cluster, Ethernet switching mode configurations do not workPR1161372
- 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 branch SRX Series 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

Network Address Translation (NAT)

- On high-end SRX Series devices, security policies are not downloaded after performing 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 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 more sessions are required for 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 changes in this

commit will not take effect. This is caused 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 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 SRX1500 devices, when RPM probe is configured for hardware timestamp-based probes, the RPM probes will be dropped by the RPM probe source (client).PR1147156
- On high-end SRX Series devices, flowd process might crash and cause traffic outage if the SPU 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, in a rare occasion, after very long uptime (approximately above 650 days) the Network Processor (NP) component of the IO card might get stuck indeterminately.PR1175656
- On SRX Series devices, NP error occurs when service offline is enabled on NP-IOC.PR1210152
- On SRX4100 and SRX4200 devices, Layer 2 Link Aggregation Control Protocol (LACP) is not supported. PR1228371
- SRX4100 and SRX4200 does not support J-Flow Version 9 in chassis cluster configuration. PR1228375
- ISSU on SRX5600 and SRX5800 with three or more SPCs, and 6000 or more VPN tunnels configured is not supported when **Establish Immediately** is configured. The workaround is to disable **Establish Immediately** on all the tunnels before starting the ISSU procedure.PR1236056

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

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

User Authentication

- In a device identity table, certain IP belongs to multi-groups (more than 20) even when the authentication source is either Active-Directory or Clear Pass. PR1225395

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 branch 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 SRX Series devices, VPN monitoring feature is not working correctly in Junos OS Release 15.1X49-D40. Hence, it is better to avoid using it. PR1163751

Related Documentation

- New and Changed Features on page 5
- Changes in Behavior and Syntax on page 10
- Known Behavior on page 26
- Resolved Issues on page 37
- Migration, Upgrade, and Downgrade Instructions on page 44

Resolved Issues

This section lists the issues fixed in hardware and software in Junos OS Release 15.1X49-D70.

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

Resolved Issues

Authentication and Access Control

- On branch SRX Series devices with pass-through authentication, the firewall client access destination server with old browser (browser like MS-IE4/MS-IE5), the flowd process might crash on all SRX Series devices when pass-through http traffic which matches the fwauth-policy. PR1203294

Chassis Cluster

- On SRX Series devices, primary node chassis cluster LED is amber even if cluster status is normal and no Monitor-failures. PR1230502
- 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

CLI

- On SRX300, SRX1500, and vSRX devices, the command **set system internet-options tcp-mss <value>** was not working on 15.1X49 releases. This issue will be addressed in D70 and later releases. PR1213775

Flow-based and Packet-based Processing

- On SRX Series devices, when firewall filter is used on GRE interface, it will be applied to packets which are crossing the interface (will not be applied to packets which are destined to the SRX). This issue only occurs under chassis cluster mode. On standalone devices the filter is working. PR1182267
- On all SRX Series devices, RSH client communicates with RSH server. RSH ALG is enabled. RSH client transfers file to RSH server. Some last packets from the RSH server are not forwarded to the RSH client. PR1202773
- After upgrading Junos OS Release to 15.1X49-D30 or above, the CPU usage of flow-SPU might be higher than before. It only happens on IOC2/IOC3 without (sufficient) NP-cache, and when hash SPU is different than session SPU. In worst case, with extensive NAT and the majority NAT traffic are forwarded from hash SPU to session SPU, the CPU usage can be 20% higher. It only affects SRX5K platforms. It starts with Junos OS Release 15.1X49-D30. From this Release, the central point architecture is enhanced to handle higher connections per second (cps). PR1207105
- On the SRX300 Series devices, system auto recovery stops working when USB storage is disabled. PR1207964
- When SkyATP was handling a certain type of malformed traffic, core files for flowd could be generated. PR1222049

- On SRX300 Series devices without Class of Service (CoS) feature configured, forwarding performance for DSCP-marked packets may be lower than expected. PR1226977
- On all SRX Series devices, whenever a large public-key (the string size exceeds more than 1K) is added to the configuration, the delete operation of that key will cause the mgd process crash. PR1229257

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. PR1131243
- On SRX devices in chassis cluster, IRB interface does not work in switching mode. PR1199445
- On SRX1500 devices, when LACP is configured, rebooting the device can trigger “l2ald” core sometimes. PR1202370
- On SRX300 Series devices, high RE CPU is noticed when ethernet-switching is configured. This leads to a higher than expected latency for traffic originating from the device itself. This issue has no impact on transit traffic through the device. PR1206823
- On SRX Series device cluster, newly configured reth interface or new configured logical unit of a reth interface, fails to come UP showing its link status as “Down”. This happens if reth interface is specified using **ether-options** configuration under physical or child interfaces. PR1212039
- On all SRX Series devices in chassis cluster, when the reth interfaces contain a single child physical interface (has no redundancy), the action of data-plane RGs failover and then failover back might cause the sessions flowed by the single-child reth interfaces in backup state on both nodes to interrupt the traffic. PR1213584
- IRB interface can not be disabled or enabled in RPM. PR1219570
- On SRX300 Series or SRX550M running 15.1X49, when you configure **l2-learning global-mode switching** and then add an IRB interface, you might experience a sudden drop in traffic passing the SRX. PR1219584
- Secure-Wire with LACP pass-through is now supported again. It was not supported in 15.1X49-D40 when LACP termination was added to transparent-mode. PR1225654
- On VLAN tagged Ethernet frames, you cannot modify 802.1p bits for host-outbound traffic. PR1225660
- Ping to IRB interface fails when multiple interfaces are part of the IRB VLAN. PR1224469
- SRX Series devices connected to VRRP backup cannot learn VIP MAC address. PR1227725

J-Web

- On all SRX Series devices, after using J-Web it may occur that the CPU utilization on the routing-engine will stay high and does not recover. PR1201267
- While using J-Web setup wizard to select multiple port under Security Topology/Zone Setup/Edit Zone, IRB interface configuration fails. PR1205163
- J-Web setup wizard might stuck at loading while editing zone setup in Security Topology. PR1205169
- Password minimum character limit is different in CLI and and J-Web.PR1215736
- On SRX Series devices, in an existing application-set which contains a nested application-set, if an additional application is added, it removes the application-set in favor of the new application. This issue occurs only in J-Web. PR1222415
- On J-Web dashboard page, chassis cluster LED shows wrong color. PR1227908

Network Address Translation (NAT)

- On SRX Series devices, the flowd process crashes and generates core dump when you first commit a NAT configuration with minor change and later commit with major change. PR1221427

Platform and Infrastructure

- On all branch SRX Series devices, on addition or deletion of VLANs, the DHCP address will not be acquired by the client and fails from the DHCP server. PR1139495
- Configuration synchronization fails when IPsec Internal SA over control link is enabled. PR1162964
- IPv6 traffic does not get load balanced over LACP link bundle when using **enhanced-hash-key session-id** knob. PR1221393

Routing Policy and Firewall Filters

- 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. PR1182591

Unified Threat Management (UTM)

- On SRX Series devices, when UTM, Security log, or Advanced Anti-Malware Service is used, in a rare condition, a memory corruption might occur on data-plane, which results in the flowd process crash. PR1154080

User Interface and Configuration

- On all SRX Series devices, system commit synchronize is not supported, but it can be configured. If **set system commit synchronize** is configured, you will not be able to make any further configuration changes. PR1134072

VPNs

- On high-end SRX Series devices, in the IPsec VPN with certificate based authentication with newly generated key-pair, the authentication might fail during IKE negotiation. PR1146279
- On hub side, autoVPN tunnel fails to come up if establish immediately is configured. Since establish immediately is not needed on hub side, there is no impact if establish immediately is not configured on hub side. PR1160948
- On branch SRX Series devices, when non-reth interfaces are used in a cluster and there is traffic that needs to be encapsulated in GRE and then sent over an IPsec tunnel, the other peer might notice ESP packets being sent by the device with incorrect sequence numbers. PR1169537
- When using P2MP IPSec VPN tunnels with dynamic routing over tunnel, ksyncd core might be encountered after RG0 failover on previous RG0 primary node, if dynamic routing is removed from VPN tunnel prior to RG0 failover. PR1170531
- On SRX Series devices, when you use IKEv2 and agressive mode on several devices that have same external interfaces, after some time of establishment, when trying to renew phase 1, the logs show the VPN trying to use the information of the last established VPN to renew the new establishment, leading to a failure to reestablished the IPsec VPN. PR1187988
- On branch SRX Series devices in a chassis cluster, VPN-monitoring with optimized option is configured and traffic go through IPsec tunnel. VPN-monitoring status will be displayed as down after RG0 failover. PR1203723
- Configuring IPsec authentication with manual SAs can cause SRX300 Series devices to crash. PR1230491

Related Documentation

- New and Changed Features on page 5

Documentation Updates

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

- In Junos OS Release 15.1X49-D70 there are no new J-Web features in this release. The J-Web online help for this release is the same as for Release 15.1x49-D60
- Starting in 15.1X49-D70, the content from *Complete Software Guide* is available in the *Complete Documentation Set*. On the 15.1X49-D70 page, click *Complete Documentation Set* to download the zip file containing the 15.1X49-D70 Feature Guide PDFs.
- In Junos OS Release 15.1X49-D70, content from the *Junos OS CLI User Guide* is available in Junos OS 15.1 CLI User Guide. On the 15.1X49-D70 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.
- In Junos OS Release 15.1X49-D70, 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-D70 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.
- In Junos OS Release 15.1X49-D70, the *Multicast Feature Guide for Security Devices* is available in *15.1 Multicast Protocols Feature Guide for Routing Devices*. On the 15.1X49-D70 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.
- In Junos OS Release 15.1X49-D70, 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-D70 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.

- In Junos OS Release 15.1X49-D70, information about MIBs is available in SNMP MIBS Explorer. On the 15.1X49-D70 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.
- In Junos OS Release 15.1X49-70, content from the *Junos OS Standards Reference*, APIs, and scripting guides are available in *15.1 Standards Reference* and API and Scripting section ofJunos OS Release 15.1 page. On the 15.1X49-D70 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.
- In Junos OS Release 15.1X49-D70, information about system log messages is available in System Log Explorer. On the 15.1X49-D70 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.
- **Ethernet Switching and Layer 2 Transparent Mode Feature Guide for Security Devices**—Starting in Junos OS Release 15.1X49-D70, the title for Layer 2 Bridging and Transparent Mode for Security Devices Feature Guide is changed to Ethernet Switching and Layer 2 Transparent Mode Feature Guide for Security Devices. On the 15.1X49-D70 page, click **Ethernet Switching and Layer 2 Transparent Mode** to view the Ethernet Switching and Layer 2 Transparent Mode Feature Guide for Security Devices.
- Starting in Junos OS Release 15.1X49-D70, 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-D70 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-D70, content from the *Junos OS System Log Monitoring and Troubleshooting Guide for Security Devices* is available in the System Log Messages. On the 15.1X49-D70 page, click **System Log Monitoring and**

Troubleshooting Guide for Security Devices to view the *Junos OS 15.1 System Log Messages*.

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 *System Log Messages* are supported on SRX Series devices. For full, confirmed support information about SRX Series devices, refer to Feature Explorer.

Related Documentation

- New and Changed Features on page 5
- Changes in Behavior and Syntax on page 10
- Known Behavior on page 26
- Known Issues on page 32
- Resolved Issues on page 37
- Migration, Upgrade, and Downgrade Instructions on page 44

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 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.

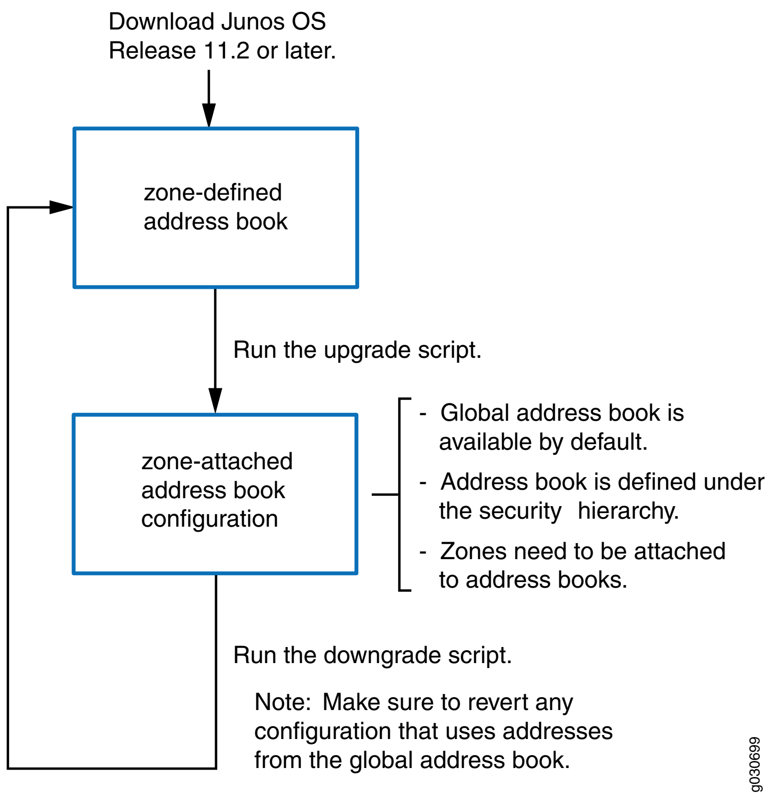
  After upgrading to the zone-attached address book configuration:

  - 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 http://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 10
- Known Behavior on page 26
- Known Issues on page 32
- Resolved Issues on page 37
- Migration, Upgrade, and Downgrade Instructions on page 44

Product Compatibility

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

- Hardware Compatibility on page 47
- Transceiver Compatibility for SRX Series Devices on page 48

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://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 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, visit us at http://www.juniper.net/support/requesting-support.html.

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 http://www.juniper.net/techpubs/feedback/.

Revision History

2, January 2018—Revision 10— Junos OS 15.1X49-D70 – SRX Series.

21, November 2017—Revision 9— Junos OS 15.1X49-D70 – SRX Series.

22, August 2017—Revision 8— Junos OS 15.1X49-D70 – SRX Series.

25, July 2017—Revision 7— Junos OS 15.1X49-D70 – SRX Series.

21, February 2017—Revision 6— Junos OS 15.1X49-D70 – SRX Series.

17, January 2017—Revision 5— Junos OS 15.1X49-D70 – SRX Series.

03, January 2017—Revision 4— Junos OS 15.1X49-D70 – SRX Series.

27, December 2016—Revision 3— Junos OS 15.1X49-D70 – SRX Series.

23, December 2016—Revision 2— Junos OS 15.1X49-D70 – SRX Series.

15, December 2016—Revision 1— Junos OS 15.1X49-D70 – SRX Series.