Release Notes: Junos® OS Release 12.3X48-D20 for the SRX Series

Release 12.3X48-D20
26 April 2017
Revision 2

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 12.3X48-D20 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/.

New and Changed Features

This section describes the new features and enhancements to existing features in Junos OS Release 12.3X48 for the SRX Series.

Release 12.3X48-D20 Software Features

Interfaces

- **CLI enhancement for interfaces operational command for SRX Series devices**—Starting with Junos OS Release 12.3X48-D20, a new **show interfaces terse zone** command is introduced. This command displays the zone name for each interface.

Screens

- **Improved logging and trapping for SRX Series devices**—Starting with Junos OS Release 12.3X48-D20, the system log information for IP-based session limits is enhanced to include more information. Each session-limit screen log now contains five tuples of information. The hard core screen SNMP trap interval can now be configured in the range from 1 second to 3600 seconds. The default interval is 2 seconds.

Security Policies

- **Setting the TCP MSS value per security policy for SRX Series devices**—Beginning with Junos OS Release 12.3X48-D20, two new options enable you to set the maximum segment size for TCP sessions per policy. The two options for the **set security policies from-zone *zone* to-zone *zone* policy *policy-name* then permit tcp-options** statement are **initial-tcp-mss *tcp-mss-value*** and **reverse-tcp-mss *tcp-mss-value***.

  Previously, a packet's maximum segment size could only be set globally, for all TCP sessions, using the **set security flow tcp-mss statement**.

  [See initial-tcp-mss, reverse-tcp-mss, and show security policies.]

VPNs

- **AutoVPN spokes and Auto Discovery VPN (ADVPN) partners supported on all high-end SRX Series devices**—Starting in Junos OS Release 12.3X48-D20, all high-end

SRX Series devices can be configured as AutoVPN spokes and ADVPN partners. In Junos OS Release 12.3X48-D10, only branch SRX Series devices were supported as ADVPN partners.

NOTE: BGP and OSPF dynamic routing protocols are supported with AutoVPN. Only OSPF is supported with ADVPN.

[See Understanding Auto Discovery VPN.]

- **IKEv2 AES-GCM for branch SRX Series and SRX5400, SRX5600, and SRX5800 devices with SPC2 (SRX5K-SPC-4-15-320)**—Starting in Junos OS Release 12.3X48-D20, support is provided for Protocol Requirements for IP Modular Encryption (PRIME), an IPsec profile defined for public sector networks in the United Kingdom. PRIME uses AES-GCM rather than AES-CBC for IKEv2 negotiations. Both PRIME-128 and PRIME-256 cryptographic suites are supported.

  The following options are available:

  - The **encryption-algorithm** options **aes-128-gcm** and **aes-256-gcm** are available for proposals configured at the [**edit security ike proposal *proposal-name***] hierarchy level.
  - Predefined proposals **prime-128** and **prime-256** are available at the [**edit security ike policy *policy-name* proposal-set**] and [**edit security ipsec policy *policy-name* proposal-set**] hierarchy levels.

  [See encryption-algorithm (Security IKE), proposal-set (Security IKE), proposal-set (Security IPsec), and Understanding Suite B and PRIME Cryptographic Suites.]

Release 12.3X48-D15 Software Features

Application Layer Gateways (ALGs)

- **464XLAT ALG traffic support for SRX Series devices**—Starting with Junos OS Release 12.3X48-D15, XLAT ALG traffic is supported for the FTP, RTSP, and PPTP ALGs. The 464XLAT architecture is a combination of stateless translation on the customer-side translator (CLAT) and stateful translation on the provider-side translator (PLAT). The 464XLAT architecture is used to translate the packet information of a device using the combination of stateless (translates private IPv4 address to global IPv6 addresses, and vice versa) and stateful (translates IPv6 addresses to global IPv4 addresses, and vice versa) translation.

  [See Understanding 464XLAT ALG Functionality and Understanding 464XLAT ALG Traffic Support.]

- **Scaling BLF support for UDP-based SIP ALG for SRX Series devices**—Starting with Junos OS Release 12.3X48-D15, the SIP ALG supports 65,000-byte SIP messages on the UDP protocol. In the scaling Busy Lamp Field (BLF) application, if every instance is around 500 bytes, the SIP ALG supports 100 instances in one SIP UDP message.

  BLF support for UDP-based SIP ALG includes the following features:

  - The device can send and receive 65,000-byte SIP messages.

- The SIP ALG can parse the 65,000-byte SIP messages and open the pinhole, if required.
- The SIP ALG regenerates the new jumbo SIP message if NAT is configured and the payload is changed.

[See Understanding Scaling Busy Lamp Field Support for the UDP-Based SIP ALG.]

Intrusion Detection Prevention (IDP)

- **New Pattern Matching Engine for SRX Series Devices**—Starting with Junos OS Release 12.3X48-D15, a new pattern matching engine is introduced for the SRX Series IDP feature. This scanning mechanism helps improve performance and policy loading.

  NOTE: **Currently, there are no changes to the existing DFA. The device continues to accept custom signatures in the existing DFA syntax.**

  [See show security idp policy-commit-status.]

Security Policies

- **Increase in number of address objects per policy for SRX3400, SRX3600, SRX5400, SRX5600, and SRX5800 devices**—Starting with Junos OS Release 12.3X48-D15, the maximum number of address objects per policy will increases from 1024 to 4096. The maximum number of policies per context for SRX3400 and SRX3600 devices will increases from 10,240 to 40,000, and for SRX5400, SRX5600, and SRX5800 devices, from 10240 to 80,000.

  [See Best Practices for Defining Policies on SRX Series Devices.]

Release 12.3X48-D10 Software Features

Application Layer Gateways (ALGs)

- **MS-RPC ALG and Sun RPC ALG map table scaling for SRX Series devices**—Starting with Junos OS Release 12.3X48-D10, the MS-RPC ALG and Sun RPC ALG dynamically allocate new mapping entries instead of using a default size (512 entries). They also offer a flexible time-based RPC mapping entry that removes the mapping entry (auto-clean) without affecting the associated active RPC sessions, including both control session and data session.

  [See Understanding Sun RPC ALGs and Understanding Microsoft RPC ALGs.]

Chassis Cluster

- **Dual active-backup IPsec VPN chassis clusters for SRX1400, SRX3400, SRX3600, SRX5600, and SRX5800 devices**—Starting with Junos OS Release 12.3X48-D10, VPN tunnels can terminate on either node of an active/active chassis cluster pair. Both nodes in the chassis cluster can actively pass traffic through VPN tunnels at the same time.

  NOTE: Z-mode flows occur when traffic enters an interface on a chassis cluster node, passes through the fabric link, and exits through an interface on the other cluster node. They are not supported with dual active-backup IPsec VPN chassis clusters.

  [See Understanding Dual Active-Backup IPsec VPN Chassis Clusters.]

Flow-based and Packet-based Processing

- **Allowing embedded ICMP packets for SRX Series devices**—Starting with Junos OS Release 12.3X48-D10, security flow allows embedded ICMP packets to pass through your device even when there is no session match. By default, an embedded ICMP packet is dropped if it does not match any session. Use the **allow-embedded-icmp** statement at the **[edit security flow]** hierarchy level to enable this feature. Once enabled, all packets encapsulated in ICMP pass through and no policy affects this behavior. This feature is useful when you have asymmetric routing in your network and you want to use traceroute and other ICMP applications on your device.

  [See allow-embedded-icmp.]

- **Enhanced security flow session command for SRX Series devices**—Starting with Junos OS Release 12.3X48-D10, the following updates have been made to the **show security flow session** command:

  - A new option, **policy-id**, allows you to query the flow session table by policy ID.
  - New output flags have been added in the command output. The three available flags are **flag**, **natflag1**, and **natflag2**.

  [See show security flow session and show security flow session policy-id.]

- **Express Path (formerly known as services offloading) on the SRX5000 line MPC for SRX5400, SRX5600, and SRX5800 devices**—Starting with Junos OS Release 12.3X48-D10, the SRX5K-MPC supports Express Path. Express Path is a mechanism for processing fast-path packets in the Trio chipset instead of in the SPU. This method reduces the long packet-processing latency that arises when packets are forwarded from network processors to SPUs for processing and back to IOCs for transmission.

  The following features are supported:

  - Support inter- and intra-Packet Forwarding Engine Express Path for IPv4
  - Per-wing statistics counter of bytes and packets sent out over the wing
  - LAG interfaces

- NAT for IPv4
- Active and backup chassis cluster

NOTE: The services offloading feature is renamed to *Express Path* starting in Junos OS Release 12.3X48-D10. Currently, the documents still use the term *services offloading*.

[See Services Offloading Overview.]

- **Improved session close log for SRX Series devices**—Starting with Junos OS Release 12.3X48-D10, the session closed log message has been expanded to include information about the device sending the TCP RST. The new log message **session closed TCP [client | server] RST** simplifies troubleshooting by indicating whether it was the client or the server that sent the TCP RST.

```
Jan 12 13:51:04 user@host RT_FLOW: RT_FLOW_SESSION_CLOSE: session closed TCP
SERVER RST: 30.0.0.2/54584->50.0.0.2/8081 None 30.0.0.2/54584->50.0.0.2/8081
None None None None 6 p1 green red 250003018 1(60) 1(40) 2 UNKNOWN UNKNOWN
N/A(N/A) ge-11/0/0.0 UNKNOWN

Jan 12 13:53:44 user@host RT_FLOW: RT_FLOW_SESSION_CLOSE: session closed TCP
CLIENT RST: 30.0.0.2/46488->50.0.0.2/23 junos-telnet 30.0.0.2/46488->50.0.0.2/23
None None None None 6 p1 green red 240003072 2(100) 1(60) 2 UNKNOWN UNKNOWN
N/A(N/A) ge-11/0/0.0 UNKNOWN
```

[See Junos OS System Log Reference for Security Devices.]

General Packet Radio Service (GPRS)

- **GTP GSN table ager for high-end SRX Series devices**—Starting with Junos OS Release 12.3X48-D10, one SRX Series device supports 100,000 GSN entries per SPU and 250,000 GSN entries per CP. Prior to this release, each entry was saved permanently. To prevent GSN entry exhaustion caused by frequent short-time roaming among countries, visiting GSNs are recorded when subscribers access the home GPRS core network from visiting countries. These entries are not deleted when the subscribers return home, but no further traffic is passed. The GTP GSN table ager causes the idling GSN entries to time out, preventing inactive GSNs from taking up too much space.

  [See show security gprs gtp gsn statistics.]

- **SCTP association scaling for high-end SRX Series devices**—Starting with Junos OS Release 12.3X48-D10, the capacity of SCTP is enhanced from 5000 associations to 20,000 associations per SPU.

  [See Understanding Stream Control Transmission Protocol.]

IP Tunneling

- **IPv6 tunneling control for SRX Series devices**—Starting with Junos OS Release 12.3X48-D10, the IPv6 tunneling control feature introduces new screens for tunneled traffic based on user preferences. By default, all tunneling traffic is allowed by the

screens unless the external IP encapsulation matches the block criteria of any existing screen. You must enable the screens to control, allow, or block the transit of tunneled traffic. The following new screens are introduced in this feature:

- GRE 4in4 Tunnel
- GRE 4in6 Tunnel
- GRE 6in4 Tunnel
- GRE 6in6 Tunnel
- Bad Inner Header Tunnel
- IPinIP 6to4relay Tunnel
- IPinIP 6in4 Tunnel
- IPinIP 6over4 Tunnel
- IPinIP 4in6 Tunnel
- IPinIP ISATAP Tunnel
- IPinIP DS-Lite Tunnel
- IPinIP 6in6 Tunnel
- IPinIP 4in4 Tunnel
- IPinUDP Teredo Tunnel

[See Understanding Screen IPv6 Tunneling Control.]

IPv6

- **Transparent mode for IPv6 support extended for SRX Series devices**—The Transparent mode for IPv6 was supported on all high-end SRX Series devices. Starting with Junos OS Release 12.3X48-D10, transparent mode for IPv6 is also supported on all branch SRX Series devices.

  [See Understanding IPv6 Flows in Transparent Mode.]

Layer 2 Features

- **Secure wire mode and mixed mode (Layer 2 and Layer 3) support for SRX Series devices**—Starting with Junos OS Release 12.3X48-D10, secure wire mode and mixed mode are supported and the interface type of these modes is the same without cross talk. You can configure both Layer 2 and Layer 3 interfaces simultaneously using separate security zones. There is no routing among IRB interfaces or between IRB interfaces and Layer 3 interfaces. Also, the user logical system is not supported for Layer 2 traffic. However, you can configure the Layer 2 interface using the root logical system.

  As with mixed mode, in secure wire mode you can configure both Layer 3 and secure wire interfaces simultaneously. In fact, you can configure Layer 3, Layer 2, and secure wire interfaces simultaneously, without traffic cross talk between any two of the three configured interfaces.

  [See Understanding Mixed Mode (Layer 2 and Layer 3).]

Network Address Translation (NAT)

- **NAT64 IPv6 prefix to IPv4 address persistent translation for SRX Series devices**—Starting with Junos OS Release 12.3X48-D10, this feature, which is targeted at IPv6 mobile networks, is used with the dual-translation mechanism, 464XLAT, to enable IPv4 services to work over IPv6-only networks. It augments the existing NAT64 mechanism, which enables IPv6 clients to contact IPv4 servers by translating IPv6 addresses to IPv4 addresses (and vice versa). However, the existing NAT64 mechanism does not ensure a sticky mapping relationship for one unique end user. By configuring the new **address-persistent** option with a specific IPv6 prefix length for NAT64 translations in an IPv4 source NAT pool, a sticky mapping relationship is ensured between one specific IPv6 prefix and one translated IPv4 address.

  [See Understanding NAT64 IPv6 Prefix to IPv4 Address-Persistent Translation.]

PKI

- **Digital certificate validation for SRX Series devices**—Starting with Junos OS Release 12.3X48-D10, the PKI daemon on SRX Series devices performs X509 certificate policy, path, key usage, and distinguished name validation, as specified in RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.

  [See Understanding Digital Certificate Validation.]

Routing Protocols

- **Virtual Router Redundancy Protocol version 3 (VRRPv3) for branch SRX Series devices**—Starting with Junos OS Release 12.3X48-D10, the Internet protocol VRRP provides one or more backup devices when a statically configured device is used on a LAN. The devices share a virtual IP address, with one device designated as the primary devices and the others as backups.

  VRRP is the combination of both IPv4 and IPv6. The VRRPv3 feature supports IPv4 and IPv6 VRRP groups, including IPv6 traps. When you configure VRRP IPV6 groups, you must set the virtual-link-local address or link-local-address value explicitly. Otherwise, the address will be automatically generated.

  To enable VRRPv3, set the **version-3** statement at the **[edit protocols vrrp]** hierarchy level.

  NOTE: To avoid having multiple primary devices in the network, the VRRPv3 IPv4 devices switch to the backup state when they receive a VRRPv2 IPv4 advertisement packet. Additionally, to avoid having multiple primary devices in your IPv6 network that are caused by checksum differences, you need to disable VRRP for IPv6 on the backup devices before you perform the VRRPv2 to VRRPv3 upgrade.

  NOTE: When you enable VRRPv3, ensure that the protocol is enabled on all the VRRP devices in the network. This is because VRRPv3 does not interoperate with previous versions of VRRP.

[See Junos OS Support for VRRPv3.]

Security

- **Secure wire interface mode and forwarding for SRX Series devices**—Starting with Junos OS Release 12.3X48-D10, secure wire allows interfaces to be mapped one-to-one for ingress-to-egress forwarding. It differs from transparent and route modes in that there is no switching or routing lookup to forward traffic. Policies and upper-layer security features permit traffic to be forwarded through the device.

  This feature is available on Ethernet logical interfaces; both IPv4 and IPv6 addresses are supported. You can configure interfaces for access or trunk mode. Secure wire supports chassis cluster redundant Ethernet interfaces and virtual LAN tagging, but it does not support IRB interfaces. This feature does not support security features not supported in transparent mode, including NAT and IPsec VPN. It does support Layer 7 features, including AppSecure, IPS, and UTM.

  [See Understanding Secure Wire.]

Unified Threat Management (UTM)

- **Redirect Web filtering support for SRX Series devices**—The redirect Web filtering solution intercepts HTTP requests and sends them to an external URL filtering server, provided by Websense, to determine whether to block or permit the requests.

  [See Understanding Redirect Web Filtering.]

VPNs

- **Auto Discovery VPN (ADVPN) protocol for SRX Series devices**—Starting with Junos OS Release 12.3X48-D10, AutoVPN deployments can use the ADVPN protocol to dynamically establish spoke-to-spoke VPN tunnels. When passing traffic from one spoke to another spoke, the hub can suggest that the spokes establish a direct security association, or "shortcut," between each other. Shortcuts can be established and torn down dynamically, resulting in better network resource utilization and reduced reliance on a centrally located hub.

  On the hub, configure **advpn suggester** at the [**edit security ike gateway *gateway-name***] hierarchy level. On spokes, configure **advpn partner** at the [**edit security ike gateway *gateway-name***] hierarchy level. ADVPN is supported with IKEv2 only.

  [See Understanding Auto Discovery VPN.]

- **AutoVPN with traffic selectors for SRX Series devices**—Starting with Junos OS Release 12.3X48-D10, AutoVPN hubs can be configured with multiple traffic selectors. This allows hubs to advertise spoke networks with different metrics.

  This feature includes the following added functionality:

  - AutoVPN hubs with traffic selectors can be configured with the st0 interface in point-to-point mode for both IKEv1 and IKEv2.

    NOTE: Dynamic routing protocols are not supported with traffic selectors with st0 interfaces in point-to-point mode.

- Traffic selectors are configured on the hub to protect traffic to spokes. Spokes can be non-SRX Series devices.

[See Understanding AutoVPN with Traffic Selectors.]

- **Enhanced VPN support for inactive-tunnel reporting and syslog for SRX Series devices**—Starting with Junos OS Release 12.3X48-D10, the methods used for debugging issues in VPN have been enhanced to improve the process in several ways. The use of CLI per-tunnel debugging, deleting the traceoptions configuration stanza after data collection is complete, and issuing the subsequent commit command are no longer required. Debugging can now be performed through Junos OS operational commands with the following VPN enhancements:
  - Information shown in the output of the **show security ipsec inactive-tunnel** command
  - System log messages

[See Understanding Tunnel Events.]

Related Documentation

- Changes in Behavior and Syntax on page 15
- Known Behavior on page 18
- Known Issues on page 21
- Resolved Issues on page 22
- Documentation Updates on page 43
- 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 12.3X48.

Attack Detection and Prevention

- On SRX5400, SRX5600 and SRX5800 devices with an IOC2 (SRX5K-MPC) card, there is a change in the screen configuration for lookup (LU) chips. There are four LU chips in each IOC2 (SRX5K-MPC) card. If the incoming traffic exceeds the threshold value in packets per second (pps), the packets are dropped. For example, if the user specifies a threshold value of 1000 pps, each LU chip will have a configured threshold value of 250 pps. In this way, the total threshold value of 1000 pps is distributed equally among the four LU chips. As an expected result, the device threshold value is 1000 pps.
- On SRX5400, SRX5600 and SRX5800 devices, when the IOC2 (SRX5K-MPC) card is in start of file (SOF) mode, only one LU chip will function. If the incoming traffic rate exceeds the threshold value, the packets are dropped as a result of the expected behavior.

Chassis Cluster

- When an SRX Series device is operating in chassis cluster mode and encounter any IA-chip access issue in an SPC or a I/O Card (IOC), a minor FPC alarm will be activated to trigger redundancy group failover.
- Starting in Junos OS Release 12.3X48-D20, for all SRX Series devices, reth interface supports proxy ARP.

Integrated User Firewall WMIC Protocol Version

- Integrated user firewall uses NTLMv2 as the default WMIC authentication protocol for security reasons. NTLMv1 exposes the system to attacks in which authentication hashes could be extracted from NTLMv1 authentication responses

IP Tunneling Screen

- Starting with Junos OS Release 12.3X48-D10, the syslog messages **RT_SCREEN_IP** and **RT_SCREEN_IP_LS** for the IP tunneling screen have been updated to include the tunnel screen attacks and log-without-drop criteria. The following list illustrates some examples of these new system log messages for each of the tunnel types:
  - **RT_SCREEN_IP: Tunnel GRE 6in4! source: 12.12.12.1, destination: 11.11.11.1, zone name: untrust, interface name: ge-0/0/1.0, action: alarm-without-drop**
  - **RT_SCREEN_IP: Tunnel GRE 6in6! source: 1212::12, destination: 1111::11, zone name: untrust, interface name: ge-0/0/1.0, action: drop**
  - **RT_SCREEN_IP: Tunnel GRE 4in4! source: 12.12.12.1, destination: 11.11.11.1, zone name: untrust, interface name: ge-0/0/1.0, action: drop**

- **RT_SCREEN_IP_LS: [lsys: LSYS1] Tunnel GRE 6in4! source: 12.12.12.1, destination: 11.11.11.1, zone name: untrust, interface name: ge-0/0/1.0, action: alarm-without-drop**
- **RT_SCREEN_IP_LS: [lsys: LSYS1] Tunnel GRE 6in6! source: 1212::12, destination: 1111::11, zone name: untrust, interface name: ge-0/0/1.0, action: drop**
- **RT_SCREEN_IP_LS: [lsys: LSYS1] Tunnel GRE 4in4! source: 12.12.12.1, destination: 11.11.11.1, zone name: untrust, interface name: ge-0/0/1.0, action: drop**

Network Time Protocol

- Starting in Junos OS Release 12.3X48-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 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.

Screen

- In Junos OS releases earlier than Junos OS Release 12.3X48-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 12.3X48-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 Management

- Maximum number of pre-authentication SSH packets—Starting with Junos OS Release 12.3X48-D10, you can limit the number of pre-authentication SSH packets that the SSH server will accept prior to user authentication. Use the **set system services ssh max-pre-authentication-packet *value*** command to set the maximum number of pre-authentication SSH packets that the server will accept.
- 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 bridge no-packet-flooding** command, then multicast packets such as OSPFv3 hello packets are dropped.

User Interface and Configuration

- Starting with Junos OS Release 12.1X44-D45 and later releases, 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

- Starting with Junos OS Release 12.3X48-D10, multicast traffic is no longer supported on secure tunnel (st0) interfaces in Protocol Independent Multicast (PIM) point-to-multipoint mode.
- Starting with Junos OS Release 12.3X48-D10, you no longer have to configure exactly matching traffic selectors on both the IKE initiator and responder. During IKE negotiation, the responder can accept from the initiator a proposed traffic selector that is a subset of the traffic selector configured on the responder. Traffic selector flexible matches are supported for both IKEv1 and IKEv2.
- Starting with Junos OS Release 12.3X48-D10, a single traffic selector configuration can result in multiple tunnels related to that traffic selector; this is referred to as multi-SA.
- Starting with Junos OS Release 12.3X48-D20, the **hmac-sha-256-96** option is deprecated at the [**edit security ipsec proposal *proposal-name* authentication-algorithm**] and [**edit security ipsec vpn *vpn-name* manual authentication algorithm**] hierarchy levels.

Related Documentation

- New and Changed Features on page 4
- Known Behavior on page 18
- Known Issues on page 21
- Resolved Issues on page 22
- Documentation Updates on page 43
- 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 12.3X48.

Application Identification and Tracking

- The application quality of service (AppQoS) feature is supported SRX5K-40GE-SFP I/O Card (IOC) and not supported on SRX5K-MPC (IOC2).

Application Layer Gateways (ALGs)

- The 464XLAT traffic is not supported in a none PAT pool with a persistent NAT pool.
- On all SRX Series devices, you can define the Sun RPC and MS RPC mapping entry ageout value using the **set security alg sunrpc map-entry-timeout *value*** and **set security alg msrpc map-entry-timeout *value*** commands. The ageout value ranges from 1 hour to 72 hours, and the default value is 32 hours.

  If either the Sun RPC ALG or the MS-RPC ALG service does not trigger the control negotiation even after 72 hours, the maximum RPC ALG mapping entry value times out and the new data connection to the service fails.

Attack Detection and Prevention (ADP)

- On all branch SRX Series devices, the fast path bad-inner-header screen is always performed first, followed by the first path signature screen.
- 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.

Chassis Cluster

- When an SRX Series device is operating in chassis cluster mode and application identification is enabled, pre-match state application IDs are not synced to other node. If there are any failover sessions, which were still under classification, will not have any application IDs assigned. This could result in application statistics and counters mismatch.

General Packet Radio Service (GPRS)

- On all high-end SRX Series devices, unified ISSU is supported from Junos OS Release 12.1X45 to Junos OS Release 12.1X46 and from Junos OS Release 12.1X46 to Junos OS Release 12.3X48-D10. Unified ISSU is not supported from Junos OS Release 12.1X45 to Junos OS Release 12.3X48-D10.

Layer 2 Features

- On all branch SRX Series devices, you cannot configure Ethernet switching and virtual private LAN service (VPLS) using mixed mode (Layer 2 and Layer 3).
- On all branch SRX Series devices, you must reboot the device when you configure bridge domain if the bridge domain was not already configured on the device.
- On all high-end SRX Series devices, you do not have to reboot the device when you configure bridge domain.
- On all branch SRX Series devices, configuring Layer 2 Ethernet switching family in Transparent Mode for an interface is not supported.
- **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).

Network Address Translation (NAT)

- On high-end SRX Series devices, the number of IP addresses for NAT with port translation has been increased to 1M addresses since Junos OS Release 12.1X47-D10.

  The SRX5000 line, however, supports a maximum of 384M translation ports and cannot be increased. To use 1M IP addresses, you must confirm that the port number is less than 384. The following CLI commands enable you to configure the twin port range and limit the twin port number:

  - **set security nat source pool-default-twin-port-range <*low*> to <*high*>**

- **set security nat source pool sp1 port range twin-port** *<low>* **to** *<high>*

VPNs

- On a high-end SRX Series device, VPN monitoring of an externally connected device (such as a PC) is not supported. The destination IP address for VPN monitoring must be a local interface on the high-end SRX Series device.
- On SRX Series devices, configuring XAuth with AutoVPN secure tunnel (st0) interfaces in point-to-multipoint mode and dynamic IKE gateways is not supported.
- On all SRX Series devices, the **disable** option is not supported on secure tunnel (st0) interfaces.
- RIP is not supported in point-to-multipoint (P2MP) VPN scenarios including AutoVPN deployments. We recommend OSPF or IBGP for dynamic routing when using P2MP VPN tunnels.
- On SRX Series devices, configuring RIP demand circuits over VPN interfaces is not supported

Related Documentation

- New and Changed Features on page 4
- Changes in Behavior and Syntax on page 15
- Known Issues on page 21
- Resolved Issues on page 22
- Documentation Updates on page 43
- Migration, Upgrade, and Downgrade Instructions on page 44

Known Issues

This section lists the known issues in hardware and software in Junos OS Release 12.3X48-D20.

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

Class of Service (CoS)

- On SRX240H or SRX240H2 devices, because of a system performance limitation, some queues of Cos might not get enough packets when the traffic is high. PR1061350

Flow-Based and Packet-Based Processing

- On all high-end SRX Series devices, packets go out of order when the device merges the prefragmented IPv6 packets and then fragments the merged IPv6 packets. PR1090550

Layer 2 Ethernet Services

- On all SRX Series devices, if the device acts as a DHCP server using the jdhcpd process and if the DHCP client sends a discover message with a requested IP address, then the authd process uses the requested IP address to find the pool with priority. This causes the device to assign an IP address from an incorrect DHCP pool to the DHCP client when there is a DHCP pool that shares the same subnet with the requested IP address. However, it is not the expected pool of the DHCP client. PR1097909
- On all SRX Series devices, if both the DHCP client and the DHCP server (using the jdhcpd process) are enabled, then changing the DHCP-related configuration might cause the jdhcpd process to exit unexpectedly. PR1118286

Related Documentation

- New and Changed Features on page 4
- Changes in Behavior and Syntax on page 15
- Known Behavior on page 18
- Resolved Issues on page 22
- Documentation Updates on page 43
- Migration, Upgrade, and Downgrade Instructions on page 44

Resolved Issues

This section lists the issues fixed in the Junos OS main release and the maintenance releases.

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

Resolved Issues: Release 12.3X48-D20

Application Layer Gateways (ALGs)

- On all SRX Series devices with NAT and SIP ALG enabled, the NOTIFY message might incorrectly arrive earlier than the 200 OK REGISTER message, which will disrupt the state machine of the REGISTER message. The subsequent 200 OK REGISTER messages are dropped and the persistent NAT entry is not refreshed, causing the persistent NAT entry to expire. As a result, the IP address in the payload of the SIP message is not translated and the SIP call fails. PR1064708
- On all SRX Series devices with NAT configured, a memory overwrite issue occurs when the scaling RAS or H.323 traffic passes through the device and the device fails to perform NAT for RAS or H.323 traffic. As a result, the flowd process might crash. PR1084549

Authentication and Access Control

- On all high-end SRX Series devices with firewall authentication configured, an authentication entry leak on the data plane occurs when an authenticated user tries to re-authenticate. As a result, firewall authentication will not allow anymore authentication entries to be created. PR969085

Chassis Cluster

- On all high-end SRX Series devices, when GPRS tunneling protocol version 2 (GTPv2) is configured, GTPv2 might fail to create control sessions. PR1029284
- On SRX1400, SRX3400, or SRX3600 chassis cluster, if the chassis cluster fabric ports are connected through a switch, some random packets might come into the chassis cluster fabric ports. These packets are interpreted as chassis cluster packets (such as real-time objects) and are forwarded to an invalid SPU. For example, the packets are forwarded to a SPU that does not exist (depending on the interpretation of the invalid packets). The invalid chassis cluster packets cannot be forwarded to the invalid SPU. Hence, the packets will be queued on a certain network processor. When the network processor is full, all data traffic will be blocked on the ports associated with that network processor. PR1042676
- On all SRX Series devices in a chassis cluster, if sampling is configured with the **input** option on an interface, the non-first fragmented packets are dropped on the secondary node. This occurs when the fragmented packets enter the interface, traverse through the fabric interface, and finally are sent out through the secondary node (z mode). PR1054775

- On SRX5400, SRX5600, and SRX5800 devices with the SPC2 (SRX5K-SPC-4-15-320) installed, after the control plane (RG0) failover, if the RG0 and data plane groups (RG1+) are active on different nodes, then the primary Routing Engine might drop the connection with the remote SPUs (the SPUs reside on an another node, which is the Routing Engine in a secondary state). As a result, traffic outage occurs. PR1059901
- On SRX5600 and SRX5800 devices, traffic outage might occur with hardware errors (IA PIO errors). When the devices are configured in a chassis cluster, the hardware errors (IA PIO errors) do not trigger RG1+ failover. This fix is used to raise an FPC minor alarm to trigger the RG1+ to switch over for a chassis cluster. PR1080116
- On SRX5400, SRX5600, and SRX5800 devices, the warning message **Warning: If you enable this feature on 40x1GE IOC, please refer to manual for the limitation** refers only to the 40x1GE IOC card; instead it should refer to all IOC cards for SRX5400, SRX5600, and SRX5800 devices. PR1082396
- On all SRX Series devices, all interfaces of the RG0 secondary node go down when the connection between the kernel of the primary node and the ksyncd of the secondary node fails. This occurs because of the memory leak in the shared-memory process (shm-rtsdbd). PR1084660
- On all SRX Series devices in a chassis cluster, when you disable the member interface of a redundant Ethernet (reth) interface and if the interface disabling action causes redundancy group failover (for example, the only member interface under the reth interface on the primary node is disabled or the number of operating member interfaces under the reth LAGs interface on the primary node falls below the configured value of minimum-links), then the reth interface will flap. PR1111360

Class of Service (CoS)

- On all SRX Series devices, the CoS rewrite rules do not work for VPN traffic if the rules are configured with **loss priority high**. This occurs when the packets are reinjected into the IPsec tunnel encapsulation process. PR1085654

Dynamic Host Configuration Protocol (DHCP)

- On all branch SRX Series devices with a DHCPv6 client configured, when the device tries to obtain an IPv6 address through the DHCPv6 prefix delegation, the device forms an incorrect IPv6 address format. As a result, the IPv6 address allocation fails. PR1084269

Flow-Based and Packet-Based Processing

- On all high-end SRX Series devices configured with chassis cluster and logical systems (LSYS), when the session number is close to the configured LSYS session limit, sessions might not be successfully created on the secondary node. The sessions will be created on the backup flow SPUs, but not on the central point. As a result, the backup flow SPUs will keep retrying until the SPUs are successful. When this situation continues, the session limit on the secondary node's SPU will reach the maximum limit value and this will affect the new session creation.

  NOTE: The number of sessions on the secondary node SPU is usually higher than on the primary node SPU. PR1061067

- On all high-end SRX Series devices, the flowd process might crash when the multicast traffic processes the route lookup failure. PR1075797
- On SRX240, SRX550, and SRX650 devices with integrated user firewall authentication configured, when you attempt to remove the user entry from the authentication table, the flowd process might crash. PR1078801
- On all branch SRX Series devices, the link-local packets for IPv4 (169.254.0.0/16) and IPv6 (fe80::/10) addresses are dropped. There is no configuration option available to change this behavior and forward the link-local packets. PR1078931
- On all SRX Series devices with source NAT configured, the ICMP error packets with 0 value of MTU might be generated on the egress interface when the packets fail to match the NAT rules. PR1079123
- On all SRX Series devices, if there are any configuration changes made to the interface (for example, when you add a new unit for an interface), an internal interface-related object will be freed and reallocated. However, in a rare condition, some packets queued in the system might refer to the freed object, causing the flowd process to crash. PR1082584
- On all SRX Series devices with integrated user firewall configured, when the user group is specified under the **source-identity** match criteria even though the valid user entry

exists in the **active-directory-authentication-table**, the traffic fails to match the security policy for the user who belongs to that user group. PR1084826

- On all high-end SRX Series devices, the flowd process might crash because of a 64-bit unaligned memory access. PR1085153
- On all SRX Series devices, if 1:1 sampling is configured for J-FLOW, and when the device processes high volume traffic, a race condition of an infinite loop of J-Flow entry deleting might be encountered, which results in the flowd process crash. PR1088476
- On all SRX Series devices, if the **inactivity-timeout** value of an application is more than 65,535, only the 16-bit value is used to calculate the **inactivity-timeout** value, which causes the application sessions to expire unexpectedly. PR1093629
- On all SRX Series devices working in transparent mode, the OSPFv3 packets are dropped when they pass through the device and are inspected by a deep packet inspection (DPI) function. PR1094093
- On all branch SRX Series devices, the **maximum-sessions** value is not displayed correctly. PR1094721
- On all SRX Series devices, if Services Offloading is enabled, in certain cases, such as packets flowing on an LAG interface or fragmented packets processing, duplicated packets might be randomly generated and forwarded out of the device. PR1104222
- On all branch SRX Series devices, in a GRE over IPsec VPN scenario, if VPN is deactivated on one side, the outgoing interface of the GRE session on the other side changes to the default route outgoing interface and does not return to the secure tunnel (st0) interface even when VPN is activated. PR1113942
- On all SRX Series devices (except the SRX110) in a chassis cluster, when ECMP is configured across the interfaces on both nodes, packets are dropped intermittently. PR1123543

Infrastructure

- On all branch SRX Series devices with health monitor configured for Routing Engine, the system health management process (syshmd) might crash due to a memory corruption in some rare conditions, such as in the scenario that concurrent conflicting manipulation of the file system occurs. PR1069868
- On SRX100, SRX110, and SRX210 devices, when you use Sierra Wireless USB 3G modem to connect to the network, Junos Space (or other Network Management devices) might fail to discover the SRX Series devices. This is because the Sierra Wireless USB 3G modem generates a duplicate address that causes the failure. PR1070898

Interfaces and Chassis

- On SRX100, SRX110, SRX210 devices with 3G or 4G USB cellular modems, sometimes the 3G or 4G connection is unstable and does not reconnect when the connection drops. PR1040125
- On SRX550 and SRX650 devices, when you insert an SFP into a GPIM, the self-traffic is delayed while the chassis reads the SFP data. This might cause a flap for protocols with aggressive timers, such as BFD or BGP. PR1043983
- On all branch SRX Series devices, when the underlying interface of the PPPoE interface is a reth interface, there is a delay of 10 seconds in displaying the PPPoE interface information when you run the **show interfaces pp*.*** command. As a result, a slower response time for the SNMP command related to the PPPoE interface is also observed. PR1068025
- On all branch SRX Series devices, if an aggregated Ethernet interface (ae) is configured as a Layer 2 interface, traffic might only be forwarded on one child interface of the ae interface. PR1074097
- On all branch SRX Series devices, the flowd process might crash when the port of the Mini-Physical Interface Module (Mini-PIM) is enabled and configured as a trunk. PR1076843
- On all branch SRX Series devices, if the **flexible-vlan-tagging** option is configured on an underlying interface of a PPPoE interface (the logical interface), the **native-vlan** option is not supported. Traffic being sent out from the logical interface that has the **native-vlan** option configured will incorrectly contain the VLAN tag. PR1084572

Intrusion Detection and Prevention (IDP)

- On all SRX Series devices, the IDP exempt rule does not work when a source or destination zone is configured as a specific zone (instead of **any**), and if one or more IP addresses are configured to match the exempt rule and an attack traffic flow (destined to IP addresses that are configured to match the exempt rule) is for a standard application on a non-standard port (for example, HTTP ports other than 80). PR1070331
- On all branch SRX Series devices with 2 GB of RAM, the maximum data segment size of the idpd process is limited to 200 million. Because of this limitation, the IDP policy compilation might fail. To avoid this issue, increase the maximum data segment size to 512 million. PR1111946

J-Web

- On all branch SRX Series devices in a chassis cluster, you cannot set the password with special characters such as !, @, #, $, %, ^, ", and so on using the J-Web chassis cluster wizard. PR1084607
- On all SRX Series devices, when you log in to J-Web using the logical system through Internet Explorer, the **Exception in data refresh** error might be displayed in the J-Web Dashboard messages log. PR1096551

- On all SRX Series devices, changing other ALG configuration through J-Web would cause IKE-ESG ALG configuration to be changed. PR1104346
- On all SRX Series devices in J-Web, the **default** option under **Security > Logging > Application Tracking** is enabled. This setting enables application tracking if any system log configuration is saved. PR1106629
- On all high-end SRX Series devices, when a logical system (LSYS) user logs in to J-Web, changes the configuration, and clicks the Compare button, the result window does not pop up. PR1115191

Network Address Translation (NAT)

- On all branch SRX Series devices in a chassis cluster, the H.323 ALG might not work properly after the chassis cluster failover. This is because the ALG binding synchronization message fails to synchronize the secondary device. PR1082934
- On all SRX Series devices, when the NAT configuration changes are made, the flowd process might crash. As a result, the memory allocation is affected. PR1084907
- On all SRX Series devices, the entry's timeout value of ALG is configured larger than the timer wheel's maximum timeout value (7200 seconds). However, this entry cannot be inserted into the timer wheel. As a result, an ALG persistent NAT binding leak occurs. PR1088539
- On all SRX Series devices, when domain names are used as a matching condition on security policies, the device sends the resolved request to the DNS server. If the DNS server is not reachable, the device tries to re-send the request to the DNS server. As a result, all the file descriptors on the nsd process become exhausted. PR1089730
- On all high-end SRX Series devices, security policies are not downloaded after ISSU from Junos OS Release 12.1X46-D40 to Junos OS Release 12.3X48-D15. PR1120951

Network Management and Monitoring

- On all SRX Series devices, when using point-to-multipoint (P2MP) automatic NHTB IPsec tunnels, routes using next-hop IP that is in the st0.x subnet are incorrectly marked as active prior to the VPN tunnel establishment. PR1042462
- On all high-end SRX Series devices in a chassis cluster, when you reboot the primary node using the **request system reboot** command, the secondary node might crash after a few seconds. PR1077626

Platform and Infrastructure

- On all SRX Series devices, the oid ifSpeed of interface which is polled by SNMP would be displayed incorrectly when the speed is configured as auto-negotiated. PR967369
- On SRX550 and SRX650 devices, 20 to 40 percent traffic loss is seen on the port of the SRX-GP-2XE-SFP-PTX after changing the speed from 10 GB to 1 GB. This issue is seen in both fiber and copper mode. When you switch between fiber and copper mode on the port of the SRX-GP-2XE-SFP-PTX, the speed might vary within the configuration. PR1033369

- On all SRX Series devices, the secondary node in a chassis cluster environment might crash or go into DB mode, displaying the **panic:rnh_index_alloc** message. This issue is sometimes observed in a chassis cluster environment with multipoint st0.x interface configured, and the tunnel interfaces flaps according to IPsec **idle-timeout** or IPsec **vpn-monitor**. PR1035779
- On SRX240 devices, after a system reboot, the link state of a VLAN interface might go down. PR1041761
- On SRX5400, SRX5600, and SRX5800 devices, an ICMP out error message is generated at the rate of 10,000 per second when you run the **show snmp mib get decimal 1.3.6.1.2.1.5.15.0** command. PR1063472
- On all branch SRX Series devices, a new version of boot loader (u-boot version 2.8) is included in the Junos OS. This new u-boot version contains a fix specifically for SRX210HE2 devices that prevents the device from failing to boot in case of flash corruption. Note that the new u-boot will not be automatically installed but will be available for upgrade, which can be confirmed by using the **show system firmware** command. PR1071560
- On SRX1400, SRX3400, and SRX3600 devices in a chassis cluster, traffic fails to flow between logical systems (LSYSs) when the secondary node goes offline. PR1073068
- On all branch SRX Series devices, in the scenario of MPLS over GRE, the MPLS traffic might fail to pass through the GRE tunnel after a system reboot. PR1073733
- On all SRX Series devices, when SNMPv3 privacy and authentication passwords are set and updated, NSM fails to push the update to the device that is managed by NSM. PR1075802
- On all SRX Series devices, when you use UTF-8 encoding to generate the certificate with the certificate authority (CA), certificate validation fails. PR1079429
- On SRX1400 devices with jumbo frames and low interpacket gaps, the interface (ge-0/0/0 to ge-0/0/5) reports Jabber or code violation errors, resulting in traffic loss. PR1080191
- On SRX550 and SRX650 devices, if a port of an 8-Port Gigabit Ethernet SFP XPIM card is set to the Ethernet switching family, locally generated packets might be dropped by the port. PR1082040
- On all branch SRX Series devices, if the destination interface and the next hop are configured for HTTP probes for real-time performance monitoring, the HTTP probes might not work. PR1086142
- On all SRX Series devices, the system log utility of the rtlogd process might crash when the WebTrends Enhanced Log File (WELF) format is configured for the security log. PR1086738
- On all branch SRX Series devices, the setting of Real-time Performance Monitoring (RPM) next-hop metric value does not take effect. PR1087753
- On all SRX Series devices, the kernel might crash when running the automatic script. PR1090549

- On all SRX Series devices, the OpenSSL project has published a set of security advisories for vulnerabilities resolved in the OpenSSL library. Junos OS is affected by one or more of these vulnerabilities. Refer to JSA10694 for more information. PR1095604
- On all branch SRX Series devices, upgrade to certain Junos OS versions might fail when a commit script is configured. PR1096576
- On all branch SRX Series devices, a syntax error is displayed when some unsupported commands are executed and when these commands are a part of the request support information as well. PR1101846
- On all high-end SRX Series devices, an SPU might become inaccessible from the Routing Engine because of a memory-buffer counter corruption. Because of this issue, a service outage occurs in certain scenarios, for example, when IPsec is configured with certificate-based authentification. PR1102376
- On all branch SRX Series devices, when any of the two possible power supplies (PS) is missing on the SRX650 device, it does not generate the alarm. In addition, the device is checking if any of the two power supplies is functioning correctly to provide the result in the output of the **show chassis craft-interface** command. However, for the status of the power supply, the output of the **show chassis craft-interface** is **PS** 0 instead of **PS**. PR1104842
- On all high-end SRX Series devices, starting in Junos OS Release 12.3X48-D20, the **set chassis fpc num sampling-instance name** command is required for J-Flow version 9 configuration. However, the commit fails when the **set chassis fpc num sampling-instance name** command is configured. PR1108371
- On all high-end SRX Series devices, you cannot configure more than one lt-0/0/0.x interface per logical systems (LSYS) on the following Junos OS maintenance releases:

  12.1X44-D35 through 12.1X44-D55

  12.1X46-D25 through 12.1X46-D40

  12.1X47-D10 through 12.1X47-D25

  12.3X48-D10 through 12.3X48-D15

  15.1X49-D10 through 15.1X49-D25

  You can configure more than one lt-0/0/0.x interface per LSYS if you have no interconnect LSYS configured. If the interconnect LSYS is configured, then you can have only one lt-0/0/0.x interface per LSYS. The issue is fixed in the following Junos OS maintenance releases: 12.1X44-D60, 12.1X46-D45, 12.1X47-D30, 12.3X48-D20, and 15.1X49-D30.

  PR1121888

Routing Policy and Firewall Filters

- On all high-end SRX Series devices, the pre-defined application-sets can only be invoked in root Logical System (LSYS) and it cannot be invoked in custom LSYSs. PR1075409

- On all SRX Series devices, the security policy scheduler fails to activate or deactivate policies when the daylight saving time (DST) change occurs. PR1080591

Routing Protocols

- On all SRX Series devices, If the device acts as a rendezvous point (RP) in a multicast environment and if the interface of the RP is configured in a custom logical system (LSYS) or routing instance, then the register-stop messages might be incorrectly sent out from the root LSYS or routing instance instead of from the custom LSYS or routing instance. PR1062305

Switching

- On all SRX Series devices, when you connect to the device through wireless AP the secure access port incorrectly allows access to the MAC addresses that are not in the list of allowed MAC addresses. PR587163
- On all branch SRX Series devices in a chassis cluster, if Ethernet switching is configured, because of a timing issue on the swfab interface initialization, the Layer 2 traffic might be dropped after a redundancy group 0 (RG0) failover. PR1103227

Unified Threat Management (UTM)

- On all SRX Series devices with secure wire and enhanced Web filtering configured, when the enhanced Web filtering initiates a session to the Websense server to validate the incoming request's category and if the request (the request to the Websense server) is transmitted in layer 3 mode first and then looped back to Layer 2 mode and forwarded out of the device, then this session (the session from the device to the Websense server) will not be established. This situation occurs because the reply from the Websense server only matches the session created in Layer 2 mode and does not match the session created in Layer 3 mode. PR1090622

User Interface and Configuration

- On all SRX Series devices, the packet capture function cannot be displayed through J-Web. However, the packet capture function can be disabled by using the CLI. PR1023944
- On all SRX Series devices, when you commit the traffic selector (TS) configuration, it might fail and an ffp core file might be generated. PR1089676

VPNs

- On SRX1400 devices, packets that are forwarded through the port of the SRX1K-SYSIO-GE card might be dropped due to CRC error. PR1036166
- On all SRX Series devices, the default trusted-ca list (Trusted_CAs.pem) is not supported by Junos OS. PR1044944
- On all branch SRX Series devices with dynamic VPN configured, the KMD process restarts or crashes, causing an IP address leak on the dynamic VPN address pool. PR1063085

- On all high-end SRX Series devices with IPsec VPN configured, tthe IPsec VPN tunnel might fail to reestablish after recovery tunnel flapping. This is because an old, invalid tunnel session exists on the central point. As a result, an attempt to create the new tunnel session fails.PR1070991
- On all SRX Series devices, the maximum number of characters allowed for an IKE policy name is limited to 31 bytes. Although you can configure more than 31 bytes by using the CLI, the bytes in excess of the limit are ignored on the data plane. PR1072958
- On all SRX Series devices with site-to-site IPsec VPN configured using IKEv2, if an active tunnel existed and the SRX Series device acted as the responder of IKEv2 negotiation, then the VPN peer initiating a duplicate IKEv2 Phase 2 negotiation request will cause the IPsec VPN tunnel to go to inactive state on the data plane side of the SRX Series device. PR1074418
- On all branch SRX Series devices with dynamic VPN configured, the key management process (KMD) might crash when an IKE payload with a different port number is received. PR1080326
- On all SRX Series devices with IPsec VPN configured, if the SRX Series device is the initiator and the other peer is from another vendors, the Internet Key Exchange (IKE) tunnel negotiation might not come up under certain conditions. PR1085657
- On all high-end SRX Series devices, when the **alarm-without-drop** option is configured for the UDP Flood Protection screen, packets classified as attack packets might be sent out of order. This can result in performance degradation. PR1090963
- On all high-end SRX Series devices, the output of the **show system processes resource-limits process-name pki-service** command cannot be shown correctly because of a missing file. PR1091233
- On all branch SRX Series devices, in group VPN setups, memory might leak during the gksd and gkmd processes. PR1098704
- On all branch SRX Series devices, an IPsec VPN using ESP encapsulation above the group VPN is not supported. As a result, the IPsec VPN traffic will be dropped because bad SPI packets are seen in the group VPN. PR1102816
- On all SRX Series devices, the IPsec tunnel does not come up on the data plane if both the st0 interface and the IPsec VPN configuration (which is configured in the [**security ike**] and [**security ipsec**] hierarchies) are committed in a single commit. PR1104466
- On all SRX Series devices, if redundant VPN tunnels are set up to use two different external interfaces within two different IKE gateways to connect the same VPN peer, and the RPM is configured for route failover and the VPN monitoring is configured when the primary link is down, then VPN fails to the secondary link as expected. However, when the primary link is up, VPN flapping might occur and establishment of the primary VPN tunnel might be delayed. PR1109372

Resolved Issues: Release 12.3X48-D15

Application Identification

- On all SRX series devices, when next-generation application identification is enabled and traffic is processed, intermittent high CPU utilization on data plane is observed. PR1064680

Application Layer Gateways (ALGs)

- On all SRX Series devices in a chassis cluster, with the TCP-based ALG enabled, if the TCP keepalive mechanism is used on the TCP server and client, after a data plane Redundancy Group (RG1+) failover, the keepalive message causes the mbuf to be held by ALG until the session timeout. This results in generation of a high mbuf usage alarm. Application communication failure occurs due to lack of mbuf. PR1031910
- On all SRX Series devices, if the SUN RPC traffic has the same IP address, port number, and program ID but is coming from different source zones other than the session, the traffic is dropped by the SUN RPC ALG. PR1050339
- On all SRX Series devices, the current SIP parser does not parse the quotation marks in the mime boundary, and the message body of the SIP messages might be cut off. PR1064869
- On all SRX Series devices with the MS-RPC ALG enabled, the flowd process might crash due to incorrect MS-RPC ALG parsing for the **ISystemActivator RemoteCreateInstance Response** packets. PR1066697

Chassis Cluster

- On all SRX Series devices in a chassis cluster, if the SCCP ALG enabled, the SCCP state flag might not be set properly while processing the SCCP call on the device. A related real-time object (RTO) hot synchronization might cause the flowd process to crash. PR1034722
- On all high-end SRX Series devices in a chassis cluster, the **count** option in the security policy might stop working after failover. This is because the Packet Forwarding Engine does not resend the message with policy states to the Routing Engine after failover. The policy lookup counter disappears when you run the **show security policies from-zone * to-zone * policy-name * detail |grep lookups** command. PR1063654
- On all branch SRX Series devices in a chassis cluster, if the switching fabric (swfab) interface is configured, the swfab interface incorrectly updates the state of the fabric (fab) interface. As a result, the fab interface might be stuck in the down state. PR1064005

CLI

- On all SRX Series devices, the output of the **show interfaces detail** and **show interfaces extensive** CLI commands for the SHDSL interface in EFM mode might not be displayed. PR1051641

Dynamic Host Configuration Protocol (DHCP)

- On all branch SRX Series devices, in DHCP requests, the IP TTL value is set to 1 and the DHCP option 12 is missing. PR1011406
- On all branch SRX Series devices configured as a DHCP server (using JDHCP), even though the next-server (siaddr) and tftp boot-server options are configured, the siaddr and tftp boot servers are set with the IP address as 0.0.0.0 in DHCP reply packets. PR1034735
- On all SRX Series devices, when an interface is configured as a DHCP client using the dhcpd process, if a hostname is not configured, the DHCP discover message will not be sent out and the DHCP client interface cannot fetch the IP address. PR1073443

Flow-Based and Packet-Based Processing

- On SRX5400, SRX5600, and SRX5800 devices with an IOC2 (SRX5K-MPC), configuring a sampling feature (flow monitoring) might cause high kernel heap memory usage. PR1033359
- On all branch SRX Series devices, after IDP drop action is performed on a TCP session, the TCP session timeout is not accurate. PR1052744
- On all branch SRX Series devices with IP-in-IP tunnel configured, due to incorrect configuration (routing loop caused by route change and so on), packets might be encapsulated by the IP-in-IP tunnel several times. As a result, packets are corrupted and the flowd process might crash. PR1055492
- On SRX240, SRX550, SRX650, SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, and SRX5800 devices, in a rare condition, the session might be doubly released by multiple threads during internal processing by the NAT module. As a result, the flowd process crashes. PR1058711
- On all SRX Series devices, under certain race conditions, if the interface associated with the name server is down, the flowd process might crash because UTM internal function was not configured. PR1066510
- On SRX100 devices, when the device is configured as an authentication enforcer of 802.1x, authentication from certain special supplicants might fail. This is because the software engine that processes the next-hops in the device incorrectly processes the packet coming from the supplicant with a special source MAC address. As a result, the packets are dropped. PR1067588
- On all SRX Series devices, when you run the **show security policies hit-count** command, the Routing Engine memory is overwritten, resulting in an nsd process crash. This issue occurs when security policies are not synchronised between the Routing Engine and the data plane. PR1069371

General Packet Radio Service (GPRS)

- On all high-end SRX Series devices in a mobile packet core network, with GTPv2 enabled and the device configured as a border gateway, the GTP packets might be dropped with a missing information element drop reason message. The packets are dropped because the information element check in processing the GTPv2 modify bearer request is not accurate. The check should only exist when Tracking Area Updates (TAU), Routing Area Updates (RAU), or handover are processed with a Serving Gateway (SGW) change on the S5/8 interface. PR1065958

Interfaces and Routing

- On all SRX Series devices, if there are multiple logical interfaces configured under a physical interface, the **shaping-rate** percentage configured for queue under schedulers might improperly calculate the value based on the speed of the physical interface. PR984052
- On all high-end SRX Series devices, during the ISSU process, the Packet Forwarding Engine connects and sometimes disconnects the Routine Engine. Hence, the IP resolve events sent to the Packet Forwarding Engine are ignored. When you configure multiple DNS policies after the ISSU process, some of the policies will not have IP addresses in the Packet Forwarding Engine. PR985731
- On SRX100H2, SRX110H2, SRX210H2, SRX220H2 and SRX240H2 devices, when you enable vlan tagging on interfaces and commit the configuration, the interface speed and duplex mode might cause the interface to stop processing traffic. PR1003423
- On all SRX Series devices, the **commit synchronize** command fails because the kernel socket gets stuck. PR1027898
- On all high-end SRX Series devices, in each node, there is only one Routing Engine. The RE 0 in the master node is the master Routing Engine and the RE 0 in the secondary node is the backup Routing Engine. The request system power-off both-routing-engines command powers off both the master and the backup Routing Engines simultaneously. PR1039758
- On all branch SRX Series devices with PPPoE configured, when PPPoE fails to authenticate, the software next-hop entry will leak in the data plane, gradually consuming all 64,000 software next-hop entries. When the software next-hop table is full, the following next-hop error pops up: **RT_PFE: NH IPC op 2 (CHANGE NEXTHOP) failed, err 6 (No Memory) peer_class 0, peer_index 0 peer_type 10**. PR1055882
- On all branch SRX Series devices, when the **set system autoinstallation interfaces interface-name bootp** command is configured, the autoinstallation enabled interface receives an IP address from the DHCP server and installs a default route on the data plane. If the autoinstallation enabled interface flaps, the default route might change and remain in dead state. PR1065754

Intrusion Detection and Prevention (IDP)

- On all branch SRX devices, severity for the IDP report changes from log severity to threat severity. PR1019401

J-Web

- On all branch SRX Series devices, when you use a configuration encryption, the missing rescue configuration alarm is set even when there is a saved rescue configuration. PR1057473
- On all branch SRX Series devices, when you configure J-Web setup wizard through creating new configuration and applying the same does not reflect all the configurations in a router. This displays configuration change alert and ask for committing the configuration. PR1058434
- On all SRX Series devices, if a security policy contains a tcp-options statement, modifying this security policy by using J-Web results in the loss of the tcp-options statement. This is because the tcp-options configuration is missing in the J-Web security policy configuration. PR1063593

Network Address Translation (NAT)

- On SRX5400, SRX5600, and SRX5800 devices with the SPC2 (SRX5K-SPC-4-15-320) installed, if a NAT IP address pool is configured with a large number of IP addresses (more than 56, 000), then running the **show snmp mib walk jnxJsNatSrcNumPortInuse** command causes the LACP to flap. PR1053650

Security Policies

- On all SRX Series devices, if two security policies are combined such that the whole address space is used, then the secondary security policy might fail to evaluate the traffic. PR1052426

System Logging

- On all SRX Series devices, the **flowd_octeon_hm: pconn_client_connect: Failed to connect to the server after 0 retries** message repeats in the log. PR1035936
- On all SRX Series devices, when IDP IP action log is configured for a security policy that matches a user identification, the information of the user name and roles is not updated in IP action logs. PR1055075
- On all SRX Series devices, the user or role retrieval information is not updated properly in the structured syslog format. PR1055097
- On SRX100 devices, when you run the **show snmp mib walk jnxMibs** command, the chassisd log repeatedly generates the **fru is present: out of range slot -1 for FAN** message. PR1062406
- On all branch SRX Series devices, the log displays the message **log: /kernel: veriexec: fingerprint for dev**. This is a cosmetic issue. PR1064166

Unified Threat Management (UTM)

- On all high-end SRX Series devices, due to a memory leak issue in the utmd process, the utmd process might cause control plane CPU utilization that is higher than expected even when the Unified Threat Management (UTM) feature is not enabled. The memory leak can only be triggered if there is a UTM license installed on the system. PR1027986
- On all SRX Series devices running Junos OS Release 12.3X48-D10 or later, with enhanced Web filtering configured, the connection to the Websense ThreatSeeker Intelligence Cloud will time out if **strict-syn-check** is enabled under **security flow tcp-session** hierarchy. PR1061064

VPNs

- On all high-end SRX Series devices with IPsec VPN configuration, because of a rare timing issue, the IPsec VPN traffic might be dropped due to a "bad SPI" message on the traffic-receiving side during IPsec Security Association (SA) rekey. PR1031890
- On all high-end SRX Series devices with policy-based IPsec VPN configured, deleting security policies that are associated with a VPN tunnel might result in a stale VPN tunnel remaining. In addition, the stale VPN tunnel might be associated with the newly added security policies. PR1034049
- On all high-end SRX series devices, in a tunnel over route-based IPsec VPN, GRE or IP-in-IP tunnel scenario, such as IPsec VPN over GRE tunnel, after the encapsulation of the first tunnel, the next-hop in internal processing might not be set properly to point to the second tunnel, which results in packet loss. PR1051541

Resolved Issues: Release 12.3X48-D10

Application Layer Gateways (ALGs)

- On all SRX Series devices with the SIP ALG and NAT enabled, if you place a call on hold or off hold many times, each time with different media ports, the resource in the call is used, resulting in one-way audio. Tearing down the call clears the resource, and following calls are not affected. PR1032528
- On all SRX Series devices with MSRPC ALG enabled, the flowd process might crash when ALG processes the MSRPC traffic which contains invalid Class IDs (CLSIDs) and unknown interface IDs (IIDs). PR1036574
- On all SRX Series devices with the SIP ALG and NAT enabled, the SIP ALG does not execute IP translation for the retransmitted 183 session progress messages. In this scenario, the SIP call will fail when the device receives the first 183 session progress messages without SDP information, but the retransmitted 183 session progress messages contains SDP information. PR1036650

- On all SRX Series devices, the DNS ALG does not terminate the session when a truncated DNS reply is received, so the session remains active until high timeout of 10~50 is reached. PR1038800
- On all branch SRX Series devices, SIP ALG code has been enhanced to support RFC 4566 regarding the SDP lines order and to avoid issues of no NAT in owner filed (O line) in some circumstances. PR1049469

Chassis Cluster

- On all high end SRX Series devices configured in a chassis cluster, after performing an ISSU upgrade on a chassis cluster containing IDP detector configuration, the FPCs on one node might remain in offline state. PR920216
- On SRX5400, SRX5600, and SRX5800 devices with SPC2 (SRX5K-SPC-4-15-320) cards installed, when IP spoofing is enabled, after the device under test (DUT) is rebooted, the address books in the Packet Forwarding Engine will be removed and not pushed back into the Packet Forwarding Engine. Due to this issue, IP spoofing does not work after the reboot. PR1025203
- On SRX Series devices in chassis cluster Z mode (except SRX110 device), if static NAT or destination NAT is configured, and in the NAT rule the IP address of the **incoming interface** is used as a matching condition for the **destination-address**, then the traffic matching the NAT rule is discarded. PR1040185
- On all high-end SRX Series devices in a chassis cluster when the mbuf usage is more than 80 percent, the device will automatically fail over. To avoid UTM traffic-overwhelmed system mbuf usage on the device, UTM function will be not enabled on the new session when system buf usage is as high as 75 percent. When usage is down, UTM function could still continue to run on the new session. PR1035986
- On all SRX Series devices in a chassis cluster, during control plane RG0 failover, a policy resynchronisation operation compares the policy message between the Routing Engine and the Packet Forwarding Engine. However, some fields in the security policy data message are not processed. Data for unprocessed fields might be treated differently and cause the flowd process to crash. PR1040819

CLI

- On all SRX Series devices, the configurations of group junos-defaults are lost after a configuration rollback. As a result, the **commit** command fails. PR1052925

Dynamic Host Configuration Protocol (DHCP)

- On all SRX Series devices configured as a DHCP server (using the jdhcpd process), when the DHCP server gets a new request from a client and applies an IP address from the authentication process (authd), the jdhcpd process communicates with authd twice as expected (once for the DHCP discovery message and once for the DHCP request message). If the authentication fails in the first message, the authd process will indefinitely wait for the second authentication request. However, the jdhcpd process never sends the second request, because the process detects that the first authentication did not occur. This causes memory leak on the authd process, and the memory might get exhausted, generating a core file and preventing DHCP server service. High CPU usage on the Routing Engine might also be observed. PR1042818

Flow-Based and Packet-Based Processing

- On all SRX Series devices, after a failover, there is a reroute process for each existing session on the newly active device. The reroute is delayed and is triggered by the first packet hitting an existing session. If multiple packets of the same session come in at once, and are picked up by different threads for processing, only one thread will run the reroute, while the other threads have to wait for the result before forwarding the packet. This waiting period penalizes traffic for other sessions and affects the overall throughput. Therefore, such packets will be dropped instead of waiting in order to optimize the overall system fairness and throughput. This drop does not affect newly created sessions, because that is a different data path. PR890785
- On all SRX Series devices, when composite next hop is used, RSVP session flap might cause an ifsate mismatch between the master Routing Engine and the backup Routing Engine, leading to a kernel crash on the master Routing Engine. PR905317
- On all SRX Series devices, when you configure **http-get** RPM probes to measure the website response, the probes might fail because the HTTP server might incorrectly interpret the request coming from the device. PR1001813
- On all branch SRX Series devices, I2C bus might hang due to read and write error with the same mutex and the following alarm message is displayed:

  2014-06-26 00:18:23 SAST Major SRXSME Chassis Fan Tray Failure
  2014-06-26 00:17:46 SAST Minor PEM 1 Absent
  2014-06-26 00:17:46 SAST Minor PEM 0 Absent

  PR1006074
- On all branch SRX Series devices, the USB modem link goes down if you configure the init-command-string **\n** to **** and **n** 2 characters. PR1020559
- On all multiple thread-based SRX Series devices (SRX240 and above), if IDP, AppSecure, ALG, GTP, or the SCTP feature, which is required for serialization flow processing is enabled, the device might encounter an issue where two flow threads

work on the same session at the same time for the serialization flow processing. This issue might cause memory corruption, and then result in a flowd process crash. PR1026692

- On all high-end SRX Series devices, when you forward traffic, a flowd core file is generated. PR1027306
- On all branch SRX Series devices, when you enable **flexible-vlan-tagging**, the return traffic might be dropped on the tagged interface with the following message: **packet dropped, pak dropped due to invalid l2 broadcast/multicast addr**". PR1034602
- On all SRX Series devices, when WebTrends Enhanced Log File (WELF) format is configured for the security log, the device generates very long WELF-formatted logs (for example, logs more than 1000 bytes). When the log is truncated on the Packet Forwarding Engine and sent to the Routing Engine, memory corruption occurs, causing the flowd process to crash. This issue generally occurs when UTM Web filtering is configured. PR1038319
- On all SRX Series devices, when a primary IP address of an interface changes, some IPsec tunnels terminated on that interface might go down. PR1044620

Hardware

- On all branch SRX Series devices, the message **twsi0: Device timeout on unit 1** fills the console on soft reboot. PR1050215

Installation and Upgrade

- On SRX650 devices, if the u-boot revision is 2.5 or later, installing the Junos OS release image from TFTP in loader mode fails. PR1016954
- On all high-end SRX Series devices, AES-GCM is not compatible with previous Junos OS releases. After you upgrade the Junos OS release on the VPN node (SRX Series device), the VPN tunnel that uses AES-GCM for encryption might not reboot. PR1037432

Interfaces and Routing

- On all branch SRX Series devices configured as a CHAP authentication client, in a PPPoE over ATM LLC encapsulation scenario, the connection might not be established because of an incorrect sequence of messages being exchanged with the second LNS. PR1027305
- On SRX210 and SRX220 devices, broadcast packets might not be sent to the Routing Engine after system initialization. PR1029424
- On all SRX Series devices, PIM register messages are not sent from the outgoing interface because the wrong outgoing interface is selected during route lookup. PR1031185
- On SRX1400, SRX3400, and SRX3600 devices, memory leak occurs on the Control Plane Processor (CPP) logical interfaces are deleted and the interprocess communication messages are received by the CPP. High memory usage on the CPP might be seen in an interface flapping situation. PR1059127

J-Web

- On all branch SRX Series devices, J-Web sets a limitation on the size of the configuration fetched from a device to avoid memory exhaustion. When the configuration size exceeds this limitation, J-Web fails to load the configuration on Junos OS Release 12.3X48-D10. PR1037073
- On all branch SRX Series devices, security policy log or security policy count is not displayed when the match condition is **RT_FLOW_SESSION**. PR1056947

Layer 2 Transparent Mode

- On all SRX Series devices in Layer 2 transparent mode, the flowd process might generate a core file when two packets of the same connection are received in a short time before the flow session is created, and destination MAC address lookup succeeds for these two packets. PR1025983

Network Address Translation (NAT)

- On all SRX Series devices, when source NAT is configured, the ports are allocated randomly by default. In rare circumstances, the global random port table of source pools or interfaces becomes damaged by certain services or traffic. This damage can result in low-range ports being assigned a higher priority in sessions. Ports might be reused quickly, causing application access failure. PR1006649
- On all SRX Series devices, when persistent NAT is enabled, allocation of resource (port) for an incoming session failed. The session reference count for that binding increases constantly even if no more sessions are associated with it. This results in stale entries in the persistent NAT binding table, which causes persistent NAT table exhaustion. PR1036020

Security

- OpenSSL released a Security Advisory that included CVE-2014-3566 known as the "POODLE" vulnerability. The SSL protocol 3.0 (SSLv3) uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain clear text data through a padding oracle attack. OpenSSL is upgraded to support for SSL 3.0 fallback protection (TLS_FALLBACK_SCSV). Refer to JSA10656 for more information. PR1033938

System Logging

- On all high-end SRX Series devices, if the stream mode logging has incomplete configuration for multiple streams, after reboot the system might not send out stream logs to the properly configured streams. PR988798

Unified Threat Management (UTM)

- On all SRX Series devices, when UTM Sophos antivirus is enabled and a file that is not supported by Sophos antivirus is transferred through SMTP, the device might not be able to handle the last packet, and mail will be on hold. When packets are later sent on this session, the packet that was on hold will be handled by the device and the system will return to normal state. PR1049506

VPNs

- On all SRX Series devices, a certificate-based IKEv2 tunnel cannot be set up if remote identity is configured as wildcard (*) for the IKE gateway. PR968614
- On SRX Series devices with IPsec VPN configured using IKEv1, the device can hold only two pairs of IPsec SA per tunnel. When the third IPsec SA rekey occurs, the oldest IPsec SA is deleted. Due to this mechanism, a looping of IPsec SA rekey might occur. For example, when a VPN peer contains incorrect configuration that has more than two proxy IDs matching only one proxy ID on a device, the rekey looping issue might cause the flowd process to crash on multiple thread-based SRX Series platforms (SRX240 devices and higher). PR996429
- On all branch SRX Series devices, in group VPN setups, all the already registered members might suddenly disappear from the key server due to memory leak. PR1023940
- On all branch SRX Series devices, when IPsec VPN is enabled using IKE version 2 and a distinguished name is used to verify the IKEv2 phase 1 remote identity, a remote peer initiates IKEv2 Phase 1 Security Association (SA) renegotiation (SRX Series devices work as responders), the new negotiated VPN tunnel might stay in "inactive" state on the data plane, causing IPsec VPN traffic loss. PR1028949
- On all branch SRX Series devices in a Dynamic End Point (DEP) VPN scenario, the VPN tunnel might stay in down state after you change the user-at-hostname value. PR1029687
- On all branch SRX Series devices, when you reboot the device in an AutoVPN configuration mode, the VPN tunnel does not come up and reports a private key error message. PR1032840

Related Documentation

- New and Changed Features on page 4
- Changes in Behavior and Syntax on page 15
- Known Behavior on page 18
- Known Issues on page 21
- Documentation Updates on page 43
- Migration, Upgrade, and Downgrade Instructions on page 44

Documentation Updates

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

IPsec VPN Feature Guide for Security Devices

- The traffic selector feature referred to as reverse route insertion (RRI) is now called auto route insertion (ARI). ARI is the automatic insertion of a static route based on the remote IP address configured in a traffic selector.

  [See Understanding Auto Route Insertion.]

Various Guides

- Content from the Feature Guides for Junos OS Release 12.3X48-D15, Junos OS Release 12.3X48-D25, and Junos OS Release 12.3X48-D30 is available in the feature-specific Guides at the Junos OS for SRX Series page.
- Some Junos OS user, reference, and configuration guides—for example the Junos Software Routing Protocols Configuration Guide, Junos OS CLI User Guide, and Junos OS System Basics Configuration Guide—mistakenly do not indicate SRX Series device support in the “Supported Platforms” list and other related support information; however, many of those documented Junos OS features are supported on SRX Series devices. For full, confirmed support information about SRX Series devices, please refer to Feature Explorer at http://pathfinder.juniper.net/feature-explorer/.

Related Documentation

Migration, Upgrade, and Downgrade Instructions

This section contains the procedure to upgrade Junos OS, and the upgrade and downgrade policies for Junos OS. Upgrading or downgrading Junos OS can take several hours, depending on the size and configuration of the network.

NOTE: Upgrading to Junos OS Release 12.1X47-D10 or later is not supported on the J Series devices or on the versions of the SRX100 and SRX200 lines with less than 2GB memory. If you attempt to upgrade one of these devices to Junos OS 12.1X47-D10 or later, installation will be aborted with the following error message:

ERROR: Unsupported platform <platform-name >for 12.1X47 and higher

For more information, refer to the Knowledge Base article at http://kb.juniper.net/TSB16632.

Network and Security Manager Support

Network and Security Manager (NSM) support for SRX Series Services Gateways with Junos OS 12.3X48-D10 is available only with NSM versions 2012.2R6 / 2012.1R10 and later. For additional information, see Network and Security Manager documentation.

Upgrading an AppSecure Device

Use the no-validate Option for AppSecure Devices.

For devices implementing AppSecure services, use the no-validate option when upgrading from Junos OS Release 11.2 or earlier to Junos OS 11.4R1 or later. The application signature package used with AppSecure services in previous releases has been moved from the configuration file to a signature database. This change in location can trigger an error during the validation step and interrupt the Junos OS upgrade. The no-validate option bypasses this step.

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.

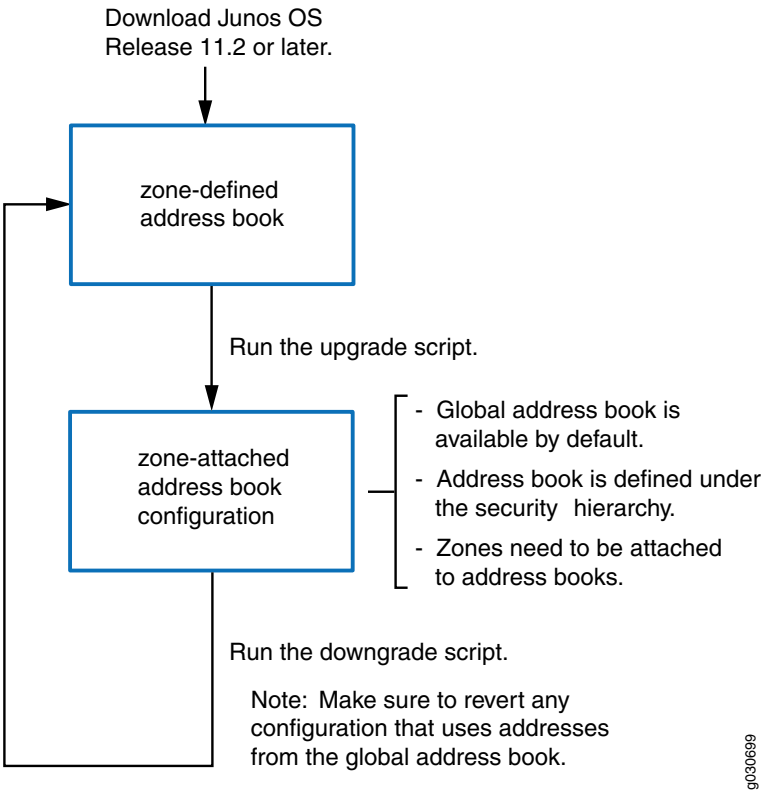
  After upgrading to the zone-attached address book configuration:

  - 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 10.0, 10.4, and 11.4 are EEOL releases. You can upgrade from Junos OS Release 10.0 to Release 10.4 or even from Junos OS Release 10.0 to Release 11.4. However, you cannot upgrade directly from a non-EEOL release that is more than three releases ahead or behind. For example, you cannot directly upgrade from Junos OS Release 10.3 (a non-EEOL release) to Junos OS Release 11.4 or directly downgrade from Junos OS Release 11.4 to Junos OS Release 10.3.

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 4
- Changes in Behavior and Syntax on page 15
- Known Behavior on page 18
- Known Issues on page 21
- Resolved Issues on page 22
- Documentation Updates on page 43

Product Compatibility

- 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.

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, fill out the documentation feedback form at http://www.juniper.net/techpubs/feedback/. 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 postsales 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/customers/support/downloads/710059.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: https://www.juniper.net/alerts/
- 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 located at https://tools.juniper.net/SerialNumberEntitlementSearch/.

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

26 April, 2017—Revision 2— Junos OS 12.3X48-D20 – SRX Series.

11 November, 2015—Revision 1— Junos OS 12.3X48-D20 – SRX Series.